On Compact Representations of Voronoi Cells of Lattices

Christoph Hunkenschröder(✉), Gina Reuland, and Matthias Schymura(✉)

École Polytechnique Fédérale de Lausanne, 1015 Lausanne, Switzerland
{christoph.hunkenschroder,matthias.schymura}@epfl.ch,
ginareuland@gmail.com

Abstract. In a seminal work, Micciancio & Voulgaris (2010) described a deterministic single-exponential time algorithm for the Closest Vector Problem (CVP) on lattices. It is based on the computation of the Voronoi cell of the given lattice and thus may need exponential space as well. We address the major open question whether there exists such an algorithm that requires only polynomial space.

To this end, we define a lattice basis to be c-compact if every facet normal of the Voronoi cell is a linear combination of the basis vectors using coefficients that are bounded by c in absolute value. Given such a basis, we get a polynomial space algorithm for CVP whose running time naturally depends on c. Thus, our main focus is the behavior of the smallest possible value of c, with the following results: There always exist c-compact bases, where c is bounded by n^2 for an n-dimensional lattice; there are lattices not admitting a c-compact basis with c growing sublinearly with the dimension; and every lattice with a zonotopal Voronoi cell has a 1-compact basis.

Keywords: Closest Vector Problem · Lattices · Voronoi cells

1 Introduction

An n-dimensional lattice is the integral linear span of n linearly independent vectors, $\Lambda = \{Bz : z \in \mathbb{Z}^n\}$, $B \in \mathbb{R}^{d\times n}$. If not stated otherwise, we always assume $d = n$, that is, the lattice has full rank.

Two widely investigated and important problems in the Algorithmic Geometry of Numbers, Cryptography, and Integer Programming are the Shortest Vector Problem and the Closest Vector Problem. Given a lattice Λ, the Shortest Vector Problem (SVP) asks for a shortest non-zero vector in Λ. For a target vector $t \in \mathbb{R}^n$, the Closest Vector Problem (CVP) asks for a lattice vector $z^\star$ minimizing the Euclidean length $\|t-z\|$ among all $z \in \Lambda$. We will only recall some milestones of the algorithmic development, for a more detailed overview we refer to the work of Hanrot, Pujol & Stehlé [15], as well as to the more recent Gaussian Sampling Algorithms, the most recent one by Aggarwal & Stephens-Davidowitz [1].

In the 1980's, Kannan presented two algorithms solving SVP and CVP in bit-complexity $n^{\mathcal{O}(n)}$ and polynomial space [17]. Although the constants involved in

A. Lodi and V. Nagarajan (Eds.): IPCO 2019, LNCS 11480, pp. 261–274, 2019.
https://doi.org/10.1007/978-3-030-17953-3_20

the running time had been improved, it took roughly fifteen years until a significantly better algorithm was discovered. In 2001, Ajtai, Kumar & Sivakumar [2] gave a randomized algorithm for the Shortest Vector Problem, only taking $2^{\mathcal{O}(n)}$ time. However, in addition to the randomness, they also had to accept exponential space dependency for their improved running time. Though their algorithm is not applicable to the Closest Vector Problem in its full generality, they show in a follow-up work that for any fixed ε, it can be used to approximate CVP up to a factor of $(1+\varepsilon)$ with running time depending on $1/\varepsilon$ [3]. These authors moreover posed the question whether randomness or exponential space is necessary for a running time better than $n^{\mathcal{O}(n)}$. It took again around a decade until this question was partially answered by Micciancio & Voulgaris [23], who obtained a deterministic $2^{\mathcal{O}(n)}$ algorithm for both problems. Their algorithm is based on computing the Voronoi cell $\mathcal{V}_\Lambda$ of the lattice, the region of all points at least as close to the origin as to any other lattice point. But as the Voronoi cell is a polytope with up to $2(2^n-1)$ facets, the Micciancio-Voulgaris algorithm needs exponential space for storing the Voronoi cell in the worst (and generic) case. Since storing the Voronoi cell in a different, "more compact," way than by facet-description would lead to a decreased space requirement, they raise the question whether such a representation exists in general.

Our main objective is to propose such a compact representation of the Voronoi cell and to investigate its merits towards a single-exponential time and polynomial space algorithm for the CVP. As being closer to the origin than to a certain lattice vector v expresses in the inequality $2\,x^\intercal v \leq \|v\|^2$, the facets of $\mathcal{V}_\Lambda$ can be stored as a set $\mathcal{F}_\Lambda \subseteq \Lambda$ of lattice vectors, which are called the *Voronoi relevant vectors*, or facet vectors. We say that a basis B of a lattice Λ is *c-compact*, if each Voronoi relevant vector of Λ can be represented in B with coefficients bounded by c in absolute value. Hence, by iterating over $(2c+1)^n$ vectors, we include the set $\mathcal{F}_\Lambda$. With $c(\Lambda)$, we denote the smallest c such that there exists a c-compact basis of Λ. As a consequence of the ideas in [23] and this notion of compactness we get (Corollary 2): Given a c-compact basis of a lattice $\Lambda \subseteq \mathbb{R}^n$, we can solve the Closest Vector Problem in time $(2c+1)^{\mathcal{O}(n)}\,\mathrm{poly}(n)$ and polynomial space.

Thus, the crucial question is: How small can we expect $c(\Lambda)$ to be for an arbitrary lattice? If $c(\Lambda)$ is constant, then the above yields asymptotically the same running time as the initial Micciancio-Voulgaris algorithm, but uses only polynomial space. Of course, this only holds under the assumption that we know a c-compact basis of Λ. This observation has consequences for the variant of CVP with preprocessing, which we discuss in Sect. 4.

As an example of a large family of lattices, we prove in Sect. 2.3, that zonotopal lattices are as compact as possible: If the Voronoi cell of Λ is a zonotope, then $c(\Lambda)=1$, and a 1-compact basis can even be found among the Voronoi relevant vectors. Moreover, every lattice of rank at most four has a 1-compact basis (see Corollary 1). However, starting with dimension five there are examples of lattices with $c(\Lambda)>1$, and thus we want to understand how large this compactness constant can be in the worst case. Motivated by applications in crystallography,

the desire for good upper bounds on $c(\Lambda)$ was already formulated in [10,11], and results of Seysen [26] imply that $c(\Lambda) \in n^{\mathcal{O}(\log n)}$. We improve this to $c(\Lambda) \leq n^2$ and, on the negative side, we identify a family of lattices without a $o(n)$-compact basis (Sects. 2.1 and 2.2).

In Sect. 3, we relax the notion of a c-compact basis as follows. Denote by $\bar{c}(\Lambda)$ the smallest constant $\bar{c}$ such that there is *any* square matrix W with $\mathcal{F}_\Lambda \subseteq \{Wz : z \in \mathbb{Z}^n,\ \|z\|_\infty \leq \bar{c}\}$. Hence, in general, the matrix W generates a superlattice of Λ. This relaxation is motivated by the fact that, given a basis, membership to a lattice can be checked in polynomial time. Thus if $\bar{c}(\Lambda)$ is much smaller than $c(\Lambda)$, this additional check is faster than iterating over a larger set. Regarding the relaxed compactness constant we prove that for every lattice Λ, we have $\bar{c}(\Lambda) \in \mathcal{O}(n \log n)$, and that there are lattices $\Lambda \subseteq \mathbb{R}^n$ with $c(\Lambda) \,/\, \bar{c}(\Lambda) \in \Omega(n)$.

In summary, our contribution can be described as follows: If we are given a $c(\Lambda)$-compact basis of a lattice, then we can modify the algorithm of Micciancio & Voulgaris to obtain a polynomial space algorithm for CVP. In whole generality, the time complexity of this algorithm cannot be better than $n^{\mathcal{O}(n)}$, as in Kannan's work. However, we provide evidence that there are large and interesting classes of lattices, for which this improves to single-exponential time. We think that it is worth to study the proposed compactness concept further. In particular, it would be interesting to understand the size of the compactness constant for a generic lattice, and to conceive an efficient algorithm to find a c-compact basis.

An extended version of this work is available on the arXiv preprint server [16].

2 The Notion of a c-compact Basis

Given a lattice $\Lambda \subseteq \mathbb{R}^n$, its *Voronoi cell* is defined by

$$\mathcal{V}_\Lambda = \{x \in \mathbb{R}^n : \|x\| \leq \|x - z\| \text{ for all } z \in \Lambda\},$$

where $\|\cdot\|$ denotes the Euclidean norm. It consists of all points that are at least as close to the origin than to any other lattice point of Λ. The Voronoi cell turns out to be a centrally symmetric polytope having outer description $\mathcal{V}_\Lambda = \left\{x \in \mathbb{R}^n : 2\,x^\intercal z \leq \|z\|^2 \text{ for all } z \in \Lambda\right\}$. A vector $v \in \Lambda$ is called *weakly Voronoi relevant* if the corresponding inequality $2\,x^\intercal v \leq \|v\|^2$ defines a supporting hyperplane of $\mathcal{V}_\Lambda$, and it is called *(strictly) Voronoi relevant* if it is moreover facet-defining. Let $\mathcal{F}_\Lambda$ and $\mathcal{C}_\Lambda$ be the set of strictly and weakly Voronoi relevant vectors of Λ, respectively. The central definition of this work is the following.

Definition 1. *A basis B of a lattice Λ is called* c-compact*, if*

$$\mathcal{F}_\Lambda \subseteq \{Bz : z \in \mathbb{Z}^n,\ \|z\|_\infty \leq c\}.$$

Moreover, the compactness constant *of Λ is defined as*

$$c(\Lambda) = \min\{c \geq 0 : \Lambda \textit{ possesses a } c\textit{-compact basis}\}.$$

As discussed in the introduction, the notion of a c-compact basis provides a compact representation of the Voronoi cell $\mathcal{V}_\Lambda$, the complexity of which depends on the value of the constant c. Before we set out to study the compactness constant in detail, we offer various equivalent definitions that serve as auxiliary tools and that also provide a better understanding of the underlying concept.

To this end, let $\Lambda^\star = \{y \in \mathbb{R}^n : y^\intercal z \in \mathbb{Z} \text{ for all } z \in \Lambda\}$ be the *dual lattice* of Λ, and let $K^\star = \{x \in \mathbb{R}^n : x^\intercal y \le 1 \text{ for all } y \in K\}$ be the *polar body* of a compact convex set $K \subseteq \mathbb{R}^n$ containing the origin in its interior. The basic properties we need are the following: If B is a basis of Λ, then $B^{-\intercal}$ is a basis of $\Lambda^\star$, usually called the *dual basis* of B. For a matrix $A \in \mathrm{GL}_n(\mathbb{R})$ and a compact convex set K as above, we have $(AK)^\star = A^{-\intercal}K^\star$. We refer to Gruber's textbook [14] for details and more information on these concepts.

Lemma 1. *Let $B = \{b_1, \dots, b_n\}$ be a basis of a lattice $\Lambda \subseteq \mathbb{R}^n$. The following are equivalent:*

(i) B is c-compact,
(ii) $c \cdot \mathrm{conv}(\mathcal{F}_\Lambda)^\star$ contains the dual basis $B^{-\intercal}$ of $\Lambda^\star$,
(iii) writing $B^{-\intercal} = \{b_1^\star, \dots, b_n^\star\}$, we have $\mathcal{F}_\Lambda \subseteq \{x \in \Lambda : |x^\intercal b_i^\star| \le c, \forall 1 \le i \le n\}$,
(iv) $\mathcal{F}_\Lambda \subseteq c\,P_B$, where $P_B = \sum_{i=1}^n [-b_i, b_i]$.

Proof. (i) $\iff$ (ii): By definition, B is c-compact if and only if $\mathcal{F}_\Lambda \subseteq \{Bz : z \in \mathbb{Z}^n, \|z\|_\infty \le c\}$. This means that $Q = \mathrm{conv}(\mathcal{F}_\Lambda) \subseteq B[-c, c]^n$. Taking polars, we see that this is equivalent to $B^{-\intercal}\frac{1}{c}C_n^\star \subseteq Q^\star$, where $C_n^\star = \mathrm{conv}\{\pm e_1, \dots, \pm e_n\}$ is the standard crosspolytope. Since the columns of $B^{-\intercal}$ constitute a basis of the dual lattice $\Lambda^\star$, the proof is finished.

(i) $\iff$ (iii): $B = \{b_1, \dots, b_n\}$ is c-compact if and only if the representation $v = \sum_{i=1}^n \alpha_i b_i$ of any Voronoi relevant vector $v \in \mathcal{F}_\Lambda$ satisfies $|\alpha_i| \le c$, for all $1 \le i \le n$. By the definition of the dual basis, we have $\alpha_i = v^\intercal b_i^\star$, which proves the claim.

(i) $\iff$ (iv): By definition, $\mathcal{F}_\Lambda \subseteq c\,P_B$ if and only if for every $v \in \mathcal{F}_\Lambda$, there are coefficients $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ such that $v = \sum_{i=1}^n \alpha_i b_i$ and $|\alpha_i| \le c$. These coefficients are unique, and since B is a basis of Λ, they are integral, that is $\alpha_i \in \mathbb{Z}$. Thus, the inclusion we started with is equivalent to saying that B is c-compact. □

Part (iv) of the above lemma shows that the compactness constant $c(\Lambda)$ is the minimum c such that $\mathcal{F}_\Lambda \subseteq c\,P_B$, for some basis B of Λ. In this definition, the concept has been introduced already by Engel, Michel & Senechal [11] together with the variant $\chi(\Lambda)$, where one replaces $\mathcal{F}_\Lambda$ by the larger set $\mathcal{C}_\Lambda$ of weakly Voronoi relevant vectors. Motivated by applications in crystallography, a reoccurring question posed in [10,11] is to give good upper bounds on these lattice invariants $c(\Lambda)$ and $\chi(\Lambda)$.

Results of Seysen [26] on simultaneous lattice reduction of the primal and dual lattice imply that $c(\Lambda) \le \chi(\Lambda) \in n^{\mathcal{O}(\log n)}$. This is however the only bound that we are aware of.

2.1 A Polynomial Upper Bound

In the sequel, we occassionally need Minkowski's *successive minima* of a convex body K and a lattice Λ in $\mathbb{R}^n$. For $1 \le i \le n$, the ith successive minimum is defined as

$$\lambda_i(K,\Lambda) = \min\{\lambda \ge 0 : \lambda K \text{ contains } i \text{ linearly independent points of } \Lambda\}.$$

Minkowski's development of his Geometry of Numbers was centered around the study of these important lattice parameters (we refer to Gruber's handbook [14] for background). With this notion, Lemma 1(ii) provides a lower bound on the compactness constant of a given lattice. Indeed, we have $c(\Lambda) \ge \lambda_n(Q^\star, \Lambda^\star)$, where $Q = \operatorname{conv}(\mathcal{F}_\Lambda)$.

Our first result aims for an explicit upper bound on $c(\Lambda)$ only depending on the dimension of the lattice. To this end, we first need an auxiliary result.

Lemma 2. *Let Λ be a lattice with Voronoi cell $\mathcal{V}_\Lambda$. Then, $\lambda_1(\mathcal{V}_\Lambda^\star, \Lambda^\star) \le \frac{2n}{\pi}$, that is, there is a dual lattice vector $y^\star \in \Lambda^\star$ such that $\mathcal{V}_\Lambda \subseteq \left\{x \in \mathbb{R}^n : |x^\intercal y^\star| \le \frac{2n}{\pi}\right\}$.*

Proof. Since $\lambda_i(\mathcal{V}_\Lambda, \Lambda) = 2$, for all $1 \le i \le n$, this follows from the transference bound $\lambda_1(\mathcal{V}_\Lambda, \Lambda)\lambda_1(\mathcal{V}_\Lambda^\star, \Lambda^\star) \le \frac{4n}{\pi}$ (cf. [18, Lem. (1.2)], [19, Cor. 1.6]). □

Theorem 1. *For every lattice $\Lambda \subseteq \mathbb{R}^n$, there exists an n^2-compact basis.*

Proof. We prove by induction on the dimension that there exists a basis $D = \{y_1, \dots, y_n\}$ of $\Lambda^\star$ such that $\mathcal{V}_\Lambda \subseteq \left\{x \in \mathbb{R}^n : |x^\intercal y_i| \le \frac{1}{2}n^2,\ 1 \le i \le n\right\}$.

Since every Voronoi relevant vector lies in the boundary of $2\mathcal{V}_\Lambda$, its inner product with each y_i is then bounded by n^2. Hence, the basis of Λ that is dual to D is an n^2-compact basis by Lemma 1(iii).

If $n = 1$, the claimed containment is trivially true, hence let $n \ge 2$. Let y_1 be a shortest vector of $\Lambda^\star$ with respect to the norm $\|\cdot\|_{\mathcal{V}_\Lambda^\star}$. By Lemma 2, we have $\mathcal{V}_\Lambda \subseteq \left\{x \in \mathbb{R}^n : |x^\intercal y_1| \le \frac{2n}{\pi}\right\}$. Let $\Lambda' = \Lambda \cap \{x \in \mathbb{R}^n : x^\intercal y_1 = 0\}$, and observe that the orthogonal projection $\pi : \mathbb{R}^n \to \{x \in \mathbb{R}^n : x^\intercal y_1 = 0\}$ fulfills $\pi(\Lambda^\star) = (\Lambda')^\star$, where we dualize with respect to the linear span of Λ' (cf. [20, Ch. 1]). By induction hypothesis, there is a basis $D' = \{y_2', \dots, y_n'\}$ of $(\Lambda')^\star$, such that $\mathcal{V}_{\Lambda'} \subseteq \left\{x \in \mathbb{R}^n : x^\intercal y_1 = 0 \text{ and } |x^\intercal y_i'| \le \frac{1}{2}(n-1)^2,\ 2 \le i \le n\right\}$. As $\Lambda' \subseteq \Lambda$, we have $\mathcal{V}_\Lambda \subseteq \mathcal{V}_{\Lambda'} + \operatorname{lin}\{y_1\}$. Moreover, as $(\Lambda')^\star$ is the projection of $\Lambda^\star$ along y_1, there exist $\alpha_i \in [-1/2, 1/2)$ such that $y_i = y_i' + \alpha_i y_1 \in \Lambda^\star$ for $2 \le i \le n$, and $D = \{y_1, \dots, y_n\}$ is a basis of $\Lambda^\star$. Hence,

$$\begin{aligned}\mathcal{V}_\Lambda &\subseteq \left\{x \in \mathbb{R}^n : |x^\intercal y_1| \le \tfrac{2n}{\pi},\ |x^\intercal y_i'| \le \tfrac{1}{2}(n-1)^2,\ 2 \le i \le n\right\}\\ &\subseteq \left\{x \in \mathbb{R}^n : |x^\intercal y_1| \le \tfrac{2n}{\pi},\ |x^\intercal y_i| \le \tfrac{1}{2}(n-1)^2 + \tfrac{n}{\pi},\ 2 \le i \le n\right\}\\ &\subseteq \left\{x \in \mathbb{R}^n : |x^\intercal y_i| \le \tfrac{1}{2}n^2,\ 1 \le i \le n\right\},\end{aligned}$$

finishing the proof. □

Remark 1. As also the weakly Voronoi relevant vectors $\mathcal{C}_\Lambda$ lie in the boundary of $2\mathcal{V}_\Lambda$, the basis from the previous proof also shows $\chi(\Lambda) \le n^2$, for every lattice Λ.

2.2 Lattices Without Sublinearly-Compact Bases

In this part, we identify an explicit family of lattices whose compactness constant grows at least linearly with the dimension. While the pure existence of such a family also follows from Proposition 4(iii) below, the class of lattices discussed in this section also allows to discriminate between the compactness constant and a relaxed variant, which will be introduced in the next section.

For any $a \in \mathbb{N}$ and $n \in \mathbb{N}$, we define the lattice

$$\Lambda_n(a) = \{z \in \mathbb{Z}^n : \ z_1 \equiv \cdots \equiv z_n \mod a\}. \tag{1}$$

As the characterization of the facet vectors, as well as the proof of the following theorem is rather technical, we refer to Appendix for the details.

Theorem 2. *Let $n \in \mathbb{N}_{\geq 4}$, $a = \lceil n/2 \rceil$. Then, the lattice $\Lambda_n = \Lambda_n(a)$ has compactness constant $c(\Lambda_n) \geq \lceil \frac{n}{4} \rceil$.*

2.3 Compact Bases and Zonotopal Lattices

For the sake of brevity, we call a 1-compact basis of a lattice just a *compact basis*. A class of lattices that allow for a compact representation of their Voronoi cells are the lattices of *Voronoi's first kind*. They correspond to those lattices Λ that comprise the first reduction domain in Voronoi's reduction theory (see [28,29]). These lattices have been characterized in [7] by possessing an *obtuse superbasis*, which is a set of vectors $\{b_0, \ldots, b_n\} \subseteq \Lambda$ that generates Λ, and that fulfills the superbasis condition $b_0 + \ldots + b_n = 0$ and the obtuseness condition $b_i^\intercal b_j \leq 0$, for all $i \neq j$. Given an obtuse superbasis, for each Voronoi relevant vector $v \in \Lambda$ there is a strict non-empty subset $S \subseteq \{0, 1, \ldots, n\}$ such that $v = \sum_{i \in S} b_i$.

Proposition 1. *(i) Every lattice of Voronoi's first kind has a compact basis.*
(ii) Every lattice of rank at most three has a compact basis.
(iii) For $n \geq 4$, the checkerboard lattice $D_n = \{x \in \mathbb{Z}^n : \mathbf{1}^\intercal x \in 2\mathbb{Z}\}$ *is not of Voronoi's first kind, but has a compact basis.*
(iv) There exists a lattice $\Lambda \subseteq \mathbb{R}^5$ with $c(\Lambda) \geq 2$.

Proof. (i): Every obtuse superbasis contains in fact a compact basis. Indeed, using the representation of a Voronoi relevant vector above and writing $b_0 = -\sum_{i=1}^n b_i$, we get $v = \sum_{i \in S} b_i = -\sum_{i \notin S} b_i$. One of the terms does not use b_0.
(ii): Every lattice of dimension at most three is of Voronoi's first kind (cf. [7]).
(iii): Bost and Künnemann [6, Prop. B.2.6] showed that for $n \geq 4$, the lattice D_n is not of Voronoi's first kind. The set $B = \{b_1, \ldots, b_n\}$ with $b_1 = e_1 + e_n$, and $b_i = e_i - e_{i-1}$ for $2 \leq i \leq n$, is a basis of D_n. The vectors $2e_i \pm 2e_j$ are contained in $2\,D_n$, for all i, j. Hence, if $\pm v$ are the unique shortest vectors in $v + 2\Lambda$, they are of the form $\{\pm(e_i \pm e_j) : 1 \leq i < j \leq n\}$. A routine calculation shows that all these vectors are a $\{-1, 0, 1\}$-combination of the basis B.
(iv): This follows immediately from Theorem 2 with the lattice $\Lambda_5(3)$. □

We now explore to which extent these initial observations on lattices with compact bases can be generalized.

A *zonotope* Z in $\mathbb{R}^n$ is a Minkowski sum of finitely many line segments, that is, $Z = \sum_{i=1}^{r}[a_i, b_i]$, for some $a_i, b_i \in \mathbb{R}^n$. The vectors $b_1 - a_1, \ldots, b_r - a_r$ are usually called the *generators* of Z. We call a lattice *zonotopal* if its Voronoi cell is a zonotope. A generic zonotopal lattice has typically high combinatorial complexity. An explicit example is the root lattice $A_n^\star$; its zonotopal Voronoi cell is generated by $\binom{n+1}{2}$ vectors and it has exactly the maximum possible $2(2^n - 1)$ facets (cf. [8, Ch. 4 & Ch. 21]).

It turns out that every lattice of Voronoi's first kind is zonotopal, but starting from dimension four, the class of zonotopal lattices is much richer (cf. Vallentin's thesis [28, Ch. 2] and [13]). In the following, we prove that every zonotopal lattice possesses a compact basis, thus extending Proposition 1(i) significantly.

Theorem 3. *Every zonotopal lattice has a compact basis. It can be found among its Voronoi relevant vectors.*

Proof. Let Λ be a zonotopal lattice in $\mathbb{R}^n$, and let $Z = \mathcal{V}_\Lambda$ be its Voronoi cell. The general idea of our proof is the following: Using Erdahl's [12] structural results on zonotopes that tile space by translation, we can find a dicing which induces the same tiling of $\mathbb{R}^n$ as the Delaunay tiling of Λ. By the duality of the Delaunay and the Voronoi tiling this provides us with additional structure that is used to identify a compact basis among the Voronoi relevant vectors. For details we refer to the Appendix. □

Our next result is in a similar spirit. It shows that if we are able to add a zonotope to a Voronoi cell and obtain a Voronoi cell again, then the compactness constant can only decrease. For its statement, we write $Z(U) = \sum_{i=1}^{r}[-u_i, u_i]$ for the possibly lower-dimensional zonotope spanned by the set of vectors $U = \{u_1, \ldots, u_r\}$. Recall, that $\chi(\Lambda)$ denotes the compactness constant for representing the set of weakly Voronoi relevant vectors of Λ.

Proposition 2. *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice such that its Voronoi cell admits a decomposition $\mathcal{V}_\Lambda = \mathcal{V}_\Gamma + Z(U)$, for some full-dimensional lattice Γ and vectors $U \subseteq \mathbb{R}^n$. Then, we have $\chi(\Lambda) \leq \chi(\Gamma)$.*

Proof. It suffices to prove the claim for the case $r = 1$. Indeed, if $Z(U)$ is generated by more than one generator, we just repeat the process successively. Hence, in the following we assume that $\mathcal{V}_\Lambda = \mathcal{V}_\Gamma + [-u, u]$, for some non-zero vector $u \in \mathbb{R}^n$. Dutour Sikirić et al. [9, Lem. 1 & Lem. 3] give a characterization of the weakly Voronoi relevant vectors of Λ in terms of those of Γ: First of all, there is a dual lattice vector $e_u \in \Gamma^\star$ such that $\Lambda = A_u\Gamma$, where $A_u x = x + 2(e_u^\intercal x)u$, for $x \in \mathbb{R}^n$. Then, $z = A_u w \in \Lambda$ is weakly Voronoi relevant if and only if w is weakly Voronoi relevant for Γ, and $e_u^\intercal w \in \{0, \pm 1\}$.

Now, let $B = \{b_1, \ldots, b_n\}$ be a basis of Γ such that for every weakly Voronoi relevant vector $w \in \mathcal{C}_\Gamma$, we have $w = \sum_{i=1}^{n} \gamma_i b_i$, for some coefficients $|\gamma_i| \leq \chi(\Gamma)$. Thus, if $z = A_u w$ is weakly Voronoi relevant for Λ, then $z = \sum_{i=1}^{n} \gamma_i (A_u b_i)$, and $A_u B$ is a basis of Λ. As a consequence, $\chi(\Lambda) \leq \chi(\Gamma)$. □

As a corollary we settle the question on the largest possible compactness constant of a four-dimensional lattice. For the proof we refer to Appendix.

Corollary 1. *Every lattice of rank at most four has a compact basis.*

3 Relaxing the Basis Condition

The compact representation problem for the set of Voronoi relevant vectors does not need B to be a basis of the lattice Λ. In fact, it suffices that we find linearly independent vectors $W = \{w_1, \ldots, w_n\}$ that allow to decompose each Voronoi relevant vector as an integer linear combination with small coefficients, as the membership to a lattice can easily be decided by solving a system of linear equations. If the constant reduces drastically by this relaxation, the additional check is still faster.

Definition 2. *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. A set of linearly independent vectors $W = \{w_1, \ldots, w_n\} \subseteq \mathbb{R}^n$ is called* c-compact for Λ, *if*

$$\mathcal{F}_\Lambda \subseteq \{w_1 z_1 + \ldots + w_n z_n : z \in \mathbb{Z}^n,\ \|z\|_\infty \leq c\}\,.$$

We define the relaxed compactness constant *of Λ as*

$$\bar{c}(\Lambda) = \min\{c \geq 0 : \textit{there is a } c\textit{-compact set } W \textit{ for } \Lambda\}.$$

If every Voronoi relevant vector is an integral combination of W, then so is *every* lattice vector. That is, a c-compact set W for Λ gives rise to a superlattice $\Gamma = W\mathbb{Z}^n \supseteq \Lambda$. The compactness constants $\bar{c}(\Lambda)$ and $c(\Lambda)$ are related as follows.

Proposition 3. *For every lattice Λ in $\mathbb{R}^n$ and $Q = \mathrm{conv}(\mathcal{F}_\Lambda)$, we have*

$$\bar{c}(\Lambda) = \lambda_n(Q^\star, \Lambda^\star) \qquad \textit{and} \qquad \bar{c}(\Lambda) \leq c(\Lambda) \leq n\,\bar{c}(\Lambda).$$

Proof. The identity $\bar{c}(\Lambda) = \lambda_n(Q^\star, \Lambda^\star)$ follows by arguments analogous to those establishing the equivalence of (i) and (ii) in Lemma 1. The inequality $\bar{c}(\Lambda) \leq c(\Lambda)$ is a direct consequence of the definition of these parameters.

By definition of the n-th successive minimum, there are linearly independent vectors $v_1, \ldots, v_n \in (\lambda_n(Q^\star, \Lambda^\star) \cdot Q^\star) \cap \Lambda^\star$. By induction on the dimension one can show that the parallelepiped $P = \sum_{i=1}^n [0, v_i]$ contains a basis of $\Lambda^\star$. Since P is contained in $n\,\lambda_n(Q^\star, \Lambda^\star) \cdot Q^\star$, the inequality $c(\Lambda) \leq n\,\bar{c}(\Lambda)$ follows. □

While the relaxation to representing $\mathcal{F}_\Lambda$ by a set W rather than by lattice bases may reduce the respective compactness constant by $\mathcal{O}(n)$, there is still a class of lattices that show that in the worst case the relaxed compactness constant can be linear in the dimension as well. In combination with Theorem 2, the second part of the following result moreover shows that the factor n in Proposition 3 is tight up to a constant.

Proposition 4. *(i) For every lattice $\Lambda \subseteq \mathbb{R}^n$, we have $\bar{c}(\Lambda) \in \mathcal{O}(n \log n)$.*
(ii) For $a = \lceil \frac{n}{2} \rceil$, let $\Lambda_n = \Lambda_n(a)$ be the lattice defined in (1). For every $n \in \mathbb{N}$, we have $\bar{c}(\Lambda_n) \leq 3$, whereas $c(\Lambda_n) \geq \lceil \frac{n}{4} \rceil$, for $n \geq 4$.
(iii) There are self-dual lattices $\Lambda \subseteq \mathbb{R}^n$ with relaxed compactness constant $\bar{c}(\Lambda) \in \Omega(n)$.

Proof. (i) The polytope $Q = \mathrm{conv}(\mathcal{F}_\Lambda)$ is centrally symmetric, all its vertices are points of Λ, and $\mathrm{int}(Q) \cap \Lambda = \{0\}$. Therefore, we have $\lambda_1(Q, \Lambda) = 1$. Proposition 3 and the transference theorem of Banaszczyk [4] thus imply that there is an absolute constant $\gamma > 0$ such that

$$\bar{c}(\Lambda) = \lambda_n(Q^\star, \Lambda^\star) = \lambda_1(Q, \Lambda) \cdot \lambda_n(Q^\star, \Lambda^\star) \leq \gamma\, n \log n. \tag{2}$$

(ii) In view of Proposition 3, we have to find n linearly independent points of $\Lambda_n^\star$ in $3\,Q^\star$. To this end, we define $y_i := \frac{1}{a}(e_i - e_n)$, for $1 \leq i \leq n-1$. Furthermore, let $y_n = \frac{1}{a}\mathbf{1}$, if n is even, and $y_n = \left(\{\frac{1}{a}\}^{n-1}, \frac{2}{a}\right)$, if n is odd. We claim that the vectors $y_1, \ldots, y_n$ do the job. They are clearly linearly independent, and since $\Lambda_n(a)^\star = \left\{z \in \frac{1}{a}\mathbb{Z}^n : \mathbf{1}^\intercal z \in \mathbb{Z}\right\}$ they belong to Λ_n. The characterization of Voronoi relevant vectors of Λ_n in Lemma 3 allows to verify $|y_i^\intercal v| \leq 3$, for all $1 \leq i \leq n$ and $v \in \mathcal{F}_{\Lambda_n}$.
(iii) Let Λ be a self-dual lattice and let $\mathcal{V}_\Lambda$ be its Voronoi cell. Each Voronoi relevant vector $v \in \mathcal{F}_\Lambda$ provides a facet of $\mathcal{V}_\Lambda$ via the inequality $v^\intercal x \leq \frac{1}{2}\|v\|^2$, as well as a facet of $Q^\star$ via the inequality $v^\intercal x \leq 1$ (this defines indeed a facet, as v is a vertex of Q – the polar of $Q^\star$). As $\|v\| \geq \lambda_1(B_n, \Lambda)$, for every $c < \lambda_1(B_n, \Lambda)^2$, we have that $c \cdot Q^\star$ is contained in the interior of twice the Voronoi cell of $\Lambda^\star = \Lambda$, and hence contains no non-trivial dual lattice point. Therefore, $\bar{c}(\Lambda) \geq \lambda_1(B_n, \Lambda)^2$.

Conway & Thompson (see [24, Ch. 2, §9]) proved that there are self-dual lattices Λ in $\mathbb{R}^n$ with minimal norm $\lambda_1(B_n, \Lambda) \geq \left\lfloor \frac{1}{\sqrt{\pi}} \left(\frac{5}{3}\Gamma\left(\frac{n}{2}+1\right)\right)^{\frac{1}{n}} \right\rfloor$. Stirling's approximation then gives that $\bar{c}(\Lambda) \in \Omega(n)$. □

Based on the common belief that the best possible upper bound in (2) is linear in n, we conjecture that $\bar{c}(\Lambda) \in \mathcal{O}(n)$, and even $c(\Lambda) \in \mathcal{O}(n)$, for every lattice $\Lambda \subseteq \mathbb{R}^n$.

4 Algorithmic Point of View

When it comes to computing a $c(\Lambda)$-compact basis, not much is known. Lemma 1 suggests to take the polar of $\mathrm{conv}(\mathcal{F}_\Lambda)$, and then to look for a dual basis in a suitable dilate thereof. However, in order to do this, we need a description of the Voronoi relevant vectors in the first place. Therefore, we rather discuss how to incorporate an already known c-compact basis into the algorithm of Micciancio and Voulgaris [23].

Their algorithm consists of two main parts. In a preprocessing step, it computes the Voronoi cell $\mathcal{V}_\Lambda$, which can be done in time $2^{\mathcal{O}(n)}$ in a recursive manner. Given a c-compact basis B this part is immediate as B grants a superset of $\mathcal{F}_\Lambda$

by definition. Once the Voronoi cell $\mathcal{V}_\Lambda$ is computed, a vector $p \in \Lambda$ is closest to a target vector t if and only if $t - p \in \mathcal{V}_\Lambda$. In the second part, they iteratively identify a Voronoi relevant vector $v \in \mathcal{F}_\Lambda$ whose induced facet inequality $2x^\intercal v \leq \|v\|^2$ is violated by t. Replacing t by the shorter vector $t - v$ and keeping track of the successively found vectors v, yields a lattice vector $p \in \Lambda$ such that $t - p \in \mathcal{V}_\Lambda$ after finitely many steps. This technique previously known as the *iterative slicer* [27], was refined in [23] to estimate the number of necessary steps by $2^n \operatorname{poly}(n)$. More sophisticated arguments, as presented in [5] allow to further decrease the number of iterations.

Corollary 2. *Assume that we are given a c-compact basis B of a lattice $\Lambda \subseteq \mathbb{R}^n$. For any target point $t \in \mathbb{R}^n$, a closest lattice vector to t can be found in time $\mathcal{O}((2c+1)^n\, 2^n \operatorname{poly}(n))$ and space polynomial in the input size.*

Proof. Theorem 4.2 and Remark 4.4 in [23] state that a closest vector can be found in time $\mathcal{O}(|V| \cdot 2^n \operatorname{poly}(n))$, where V is a superset of the Voronoi relevant vectors $\mathcal{F}_\Lambda$. We set $V = \{Bz : z \in \mathbb{Z}^n,\ \|z\|_\infty \leq c\} \supseteq \mathcal{F}_\Lambda$.

The reduction to polynomial space follows from [23, Rem. 4.3]: Their algorithm may need exponential space because they store $\mathcal{F}_\Lambda$. As a subset of V it is however described just by the polynomial-size data (B, c). □

The Micciancio-Voulgaris algorithm naturally can be presented as an algorithm for the Closest Vector Problem with Preprocessing (CVPP). In this variant of CVP, we may precompute the lattice for an arbitrary amount of time and store some additional information. Only then the target vector is revealed to us, and the additional information can be used to find a closest vector faster. In practice, we might have to solve CVP on the same lattice with several target vectors, hence we might benefit from spending more time for preprocessing.

Considered in this setting, our results compress the information after the preprocessing step into polynomial space. However, it is unclear how to compute a c-compact basis *without* computing the Voronoi cell first.

Problem 1. Can we compute a basis B of Λ attaining $c(\Lambda)$ in single-exponential time and polynomial space?

McKilliam et al. [21] show that for lattices of Voronoi's first kind, CVP can be solved in polynomial time, provided an obtuse superbasis is known. One may wonder whether our representation also allows for solving CVPP faster. However, Micciancio [22] showed that if CVPP can be solved in polynomial time for arbitrary lattices, then NP $\subseteq$ P/poly and the polynomial hierarchy collapses.

Acknowledgments. We thank Daniel Dadush and Frank Vallentin for helpful remarks and suggestions. In particular, Daniel Dadush pointed us to the arguments in Theorem 1 that improved our earlier estimate of order $\mathcal{O}(n^2 \log n)$.

This work was supported by the Swiss National Science Foundation (SNSF) within the project *Convexity, geometry of numbers, and the complexity of integer programming (Nr. 163071)*. The paper grew out of the master thesis of the second author [25].

Appendix

Lemma 3. *Let $n \in \mathbb{N}_{\geq 4}$, $a = \lceil n/2 \rceil$, and $\Lambda_n = \Lambda_n(a)$. A vector $v \in \Lambda_n$ is Voronoi relevant if and only if $v = \pm\mathbf{1}$, or there exists $\emptyset \neq S \subsetneq \{1, \ldots, n\}$ s.t.*

$$v_i = a - \ell \ (i \in S), \quad v_j = -\ell \ (j \notin S), \quad \text{and} \quad \ell \in \{\lfloor \tfrac{a|S|}{n} \rfloor, \lceil \tfrac{a|S|}{n} \rceil\}. \tag{3}$$

Proof (Sketch). Voronoi characterized a strictly Voronoi relevant vector v in a lattice Λ by the property that $\pm v$ are the only shortest vectors in the co-set $v + 2\Lambda$ (cf. [8, p. 477]). We use this crucially to show that Voronoi relevant vectors different from $\pm\mathbf{1}$ are characterized by (3).

The vectors $\pm\mathbf{1}$ are Voronoi relevant as they are shortest vectors of the lattice; if two linearly independent shortest vectors v_1, v_2 were in the same co-set $v_1 + 2\Lambda_n$, then $(v_1 + v_2)/2$ would be a strictly shorter vector. To analyze any shortest vector u of some co-set $v + 2\Lambda_n$, $v \in \Lambda_n$, we make the following two observations. First, as $2ae_i \in 2\Lambda_n$, we have $u \in [-a, a]^n$. Due to the definition of Λ_n, either $u \in \{0, \pm a\}^n$, or $u \in [-a + 1, a - 1]^n$. In the first case, if we have at least two non-zero entries, we can flip the sign of one entry and obtain a vector of the same length in the same co-set, but linearly independent. Hence, that co-set does not have any Voronoi relevant vectors. In the other case, again due to $v_i \equiv v_j \mod a$ for any lattice vector, $u \in \{a - \ell, -\ell\}^n$ for some $1 \leq \ell < n$. Considering the norm of u as a function in ℓ and bearing in mind that $\mathbf{1} \in 2\Lambda_n$, we see that $\|u\|^2$ is minimized precisely for the choices of ℓ given in (3). Due to this line of thought, in order to show that each vector u of shape (3) is indeed Voronoi relevant, it suffices to show that any vector in $\{-a, 0, a\}^n$ is either longer than u, or in another residue class. □

Proof (Theorem 2). For brevity, we write $c = c(\Lambda_n)$, $Q = \mathrm{conv}(\mathcal{F}_{\Lambda_n})$. As $\mathbf{1} \in \Lambda_n$, there exists a $w \in \Lambda_n^\star$ with $\mathbf{1}^\intercal w = 1$, implying that each basis of $\Lambda_n^\star$ contains a vector y such that $\mathbf{1}^\intercal y$ is an odd integer. In particular, by Lemma 1, we know that $cQ^\star$ contains such a y. As $Q^\star$ is centrally symmetric, assume $\mathbf{1}^\intercal y \geq 1$. Further, since $\Lambda_n^\star$ is invariant under permutation of the coordinates, we may assume that $y_1 \geq y_2 \geq \cdots \geq y_n$. Let us outline our arguments: We split $\mathbf{1}^\intercal y$ into two parts, by setting $A := \sum_{i=1}^{k} y_i$, and $B := \sum_{i>k}^{n} y_i$, where $k = \lceil n/2 \rceil$. We show that $A \geq B + 1$, and construct a Voronoi relevant vector $v \in \Lambda_n$ by choosing $S = \{1, \ldots, k\}$ and $\ell = \lfloor ak/n \rfloor$. Hence, $(a - \ell), \ell \approx n/4$ and we obtain $v^\intercal y \gtrsim \frac{n}{4}A - \frac{n}{4}B \geq n/4$ by distinguishing the four cases $n \mod 4$.

For showing $A \geq B + 1$, consider y_k. As $y \in \Lambda_n^\star$, there is an integer z such that we can write $y_k = \frac{z}{a}$. Note that we have $A \geq k y_k = z$ and $B \leq (n-k)\frac{z}{a} \leq z$. Let $\alpha, \gamma \geq 0$ such that $A = z + \alpha$ and $B = z - \gamma$. As $A + B = 2z + \alpha - \gamma$ has to be an odd integer, we have $|\alpha - \gamma| \geq 1$, implying $\alpha \geq 1$ or $\gamma \geq 1$. Therefore, in fact we have $A \geq \max\{B + 1, 1\}$. □

We now give the details of the proof of Theorem 3. A *dicing* $\mathfrak{D}$ in $\mathbb{R}^n$ is an arrangement consisting of families of infinitely many equally-spaced hyperplanes with the following properties: (i) there are n families with linearly independent

normal vectors, and (ii) every vertex of the arrangement is contained in a hyperplane of each family. The vertex set of a dicing forms a lattice $\Lambda(\mathfrak{D})$. Erdahl [12, Thm. 3.1] represents a dicing $\mathfrak{D}$ as a set $D = \{\pm d_1, \ldots, \pm d_r\}$ of hyperplane normals and a set $E = \{\pm e_1, \ldots, \pm e_s\} \subseteq \Lambda(\mathfrak{D})$ of edge vectors of the arrangement $\mathfrak{D} = \mathfrak{D}(D, E)$ satisfying: (E1) Each pair of edges $\pm e_j \in E$ is contained in a line $d_{i_1}^{\perp} \cap \ldots \cap d_{i_{n-1}}^{\perp}$, for some linearly independent $d_{i_1}, \ldots, d_{i_{n-1}} \in D$, and conversely each such line contains a pair of edges; (E2) For each $1 \leq i \leq r$ and $1 \leq j \leq s$, we have $d_i^{\intercal} e_j \in \{0, \pm 1\}$.

Proof (Theorem 3). We start by reviewing the *Delaunay tiling* of the lattice Λ. A sphere $B_c(R) = \{x \in \mathbb{R}^n : \|x - c\|^2 \leq R^2\}$ is called an *empty sphere* of Λ (with center $c \in \mathbb{R}^n$ and radius $R \geq 0$), if every point in $B_c(R) \cap \Lambda$ lies on the boundary of $B_c(R)$. A *Delaunay polytope* of Λ is defined as the convex hull of $B_c(R) \cap \Lambda$, and the family of all Delaunay polytopes induces a tiling $\mathcal{D}_\Lambda$ of $\mathbb{R}^n$ which is the Delaunay tiling of Λ. This tiling is in fact dual to the Voronoi tiling.

Erdahl [12, Thm. 2] shows that the Voronoi cell of a lattice is a zonotope if and only if its Delaunay tiling is a dicing. More precisely, the tiling $\mathcal{D}_\Lambda$ induced by the Delaunay polytopes of Λ is equal to the tiling induced by the hyperplane arrangement of a dicing $\mathfrak{D} = \mathfrak{D}(D, E)$ with normals $D = \{\pm d_1, \ldots, \pm d_r\}$ and edge vectors $E = \{\pm e_1, \ldots, \pm e_s\}$. By the duality of the Delaunay and the Voronoi tiling, an edge of $\mathcal{D}_\Lambda$ containing the origin corresponds to a facet normal of the Voronoi cell $\mathcal{V}_\Lambda$. Therefore, the edge vectors E are precisely the Voronoi relevant vectors of Λ.

Now, choosing n linearly independent normal vectors, say $d_1, \ldots, d_n \in D$, the properties (E1) and (E2) imply the existence of edge vectors, say $e_1, \ldots, e_n \in E$, such that $d_i^{\intercal} e_j = \delta_{ij}$, with δ_{ij} being the Kronecker delta. Moreover, the set $B = \{e_1, \ldots, e_n\}$ is a basis of $\{x \in \mathbb{R}^n : d_i^{\intercal} x \in \mathbb{Z}, 1 \leq i \leq n\}$, which by property E2) equals the whole lattice Λ. Hence, $\{d_1, \ldots, d_n\}$ is the dual basis of B and every Voronoi relevant vector $v \in \mathcal{F}_\Lambda = E$ fulfills $d_i^{\intercal} v \in \{0, \pm 1\}$. In view of Lemma 1 (iii), this means that B is a compact basis of Λ consisting of Voronoi relevant vectors, as desired. □

Proof (Corollary 1). By Proposition 1(ii), every lattice of rank ≤ 3 has a compact basis. Thus, let $\Lambda \subseteq \mathbb{R}^4$ be of full rank. If Λ is zonotopal, then by Theorem 3 $c(\Lambda) = 1$. Voronoi's reduction theory shows that if Λ is not zonotopal, then its Voronoi cell $\mathcal{V}_\Lambda$ has the 24-cell as a Minkowski summand (cf. [28, Ch. 3]). Up to isometries and scalings, the only lattice whose Voronoi cell is combinatorially equivalent to the 24-cell, is the root lattice D_4. Thus, we have a decomposition $\mathcal{V}_\Lambda = \mathcal{V}_\Gamma + Z(U)$, for some generators $U = \{u_1, \ldots, u_r\} \subseteq \mathbb{R}^4$ and a lattice Γ that is isometric to D_4. Hence, by Proposition 2, we get $c(\Lambda) \leq \chi(\Lambda) \leq \chi(\Gamma) = \chi(D_4)$. Engel et al. [11] computed that $\chi(D_4) = 1$, which finishes our proof. □

References

1. Aggarwal, D., Stephens-Davidowitz, N.: Just take the average! an embarrassingly simple 2^n-time algorithm for SVP (and CVP). In: OASIcs-OpenAccess Series in Informatics, vol. 61. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik (2018). https://doi.org/10.4230/OASIcs.SOSA.2018.12
2. Ajtai, M., Kumar, R., Sivakumar, D.: A sieve algorithm for the shortest lattice vector problem. In: Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing, pp. 601–610. ACM (2001). https://doi.org/10.1145/380752.380857
3. Ajtai, M., Kumar, R., Sivakumar, D.: Sampling short lattice vectors and the closest lattice vector problem. In: Proceedings 17th IEEE Annual Conference on Computational Complexity, pp. 53–57. IEEE (2002). https://doi.org/10.1109/CCC.2002.1004339
4. Banaszczyk, W.: Inequalities for convex bodies and polar reciprocal lattices in R^n. II. Application of K-convexity. Discrete Comput. Geom. **16**(3), 305–311 (1996). https://doi.org/10.1007/BF02711514
5. Bonifas, N., Dadush, D.: Short paths on the Voronoi graph and closest vector problem with preprocessing. In: Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 295–314. SIAM, Philadelphia (2015). https://doi.org/10.1137/1.9781611973730.22
6. Bost, J.B., Künnemann, K.: Hermitian vector bundles and extension groups on arithmetic schemes I. Geometry of numbers. Adv. Math. **223**(3), 987–1106 (2010). https://doi.org/10.1016/j.aim.2009.09.005
7. Conway, J.H., Sloane, N.J.A.: Low-dimensional lattices. VI. Voronoĭ reduction of three-dimensional lattices. Proc. Roy. Soc. Lond. Ser. A **436**(1896), 55–68 (1992). https://doi.org/10.1098/rspa.1992.0004
8. Conway, J.H., Sloane, N.J.A.: Sphere packings, lattices and groups, Grundlehren der Mathematischen Wissenschaften. Fundamental Principles of Mathematical Sciences, 3rd edn., vol. 290. Springer, New York (1999). https://doi.org/10.1007/978-1-4757-6568-7
9. Dutour Sikirić, M., Grishukhin, V., Magazinov, A.: On the sum of a parallelotope and a zonotope. Eur. J. Combin. **42**, 49–73 (2014). https://doi.org/10.1016/j.ejc.2014.05.005
10. Engel, P.: Mathematical problems in modern crystallography. Comput. Math. Appl. **16**(5–8), 425–436 (1988). https://doi.org/10.1016/0898-1221(88)90232-5
11. Engel, P., Michel, L., Senechal, M.: New geometric invariants for Euclidean lattices. In: Réseaux euclidiens, designs sphériques et formes modulaires, Monogr. Enseign. Math., vol. 37, pp. 268–272. Enseignement Math., Geneva (2001)
12. Erdahl, R.M.: Zonotopes, dicings, and Voronoi's conjecture on parallelohedra. Eur. J. Combin. **20**(6), 527–549 (1999). https://doi.org/10.1006/eujc.1999.0294
13. Erdahl, R.M., Ryshkov, S.S.: On lattice dicing. Eur. J. Combin. **15**(5), 459–481 (1994). https://doi.org/10.1006/eujc.1994.1049
14. Gruber, P.M.: Convex and discrete geometry, Grundlehren der Mathematischen Wissenschaften. Fundamental Principles of Mathematical Sciences, vol. 336. Springer, Berlin (2007). https://doi.org/10.1007/978-3-540-71133-9
15. Hanrot, G., Pujol, X., Stehlé, D.: Algorithms for the shortest and closest lattice vector problems. In: Chee, Y.M., et al. (eds.) IWCC 2011. LNCS, vol. 6639, pp. 159–190. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20901-7_10

16. Hunkenschröder, C., Reuland, G., Schymura, M.: On compact representations of Voronoi cells of lattices. https://arxiv.org/abs/1811.08532 (2018)
17. Kannan, R.: Minkowski's convex body theorem and integer programming. Math. Oper. Res. **12**(3), 415–440 (1987). https://doi.org/10.1287/moor.12.3.415
18. Kannan, R., Lovász, L.: Covering minima and lattice-point-free convex bodies. Ann. Math. (2) **128**(3), 577–602 (1988). https://doi.org/10.2307/1971436
19. Kuperberg, G.: From the mahler conjecture to gauss linking integrals. Geom. Funct. Anal. **18**(3), 870–892 (2008). https://doi.org/10.1007/s00039-008-0669-4
20. Martinet, J.: Perfect lattices in Euclidean spaces, Grundlehren der Mathematischen Wissenschaften. Fundamental Principles of Mathematical Sciences, vol. 327. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-662-05167-2
21. McKilliam, R.G., Grant, A., Clarkson, I.V.L.: Finding a closest point in a lattice of Voronoi's first kind. SIAM J. Discrete Math. **28**(3), 1405–1422 (2014). https://doi.org/10.1137/140952806
22. Micciancio, D.: The hardness of the closest vector problem with preprocessing. IEEE Trans. Inform. Theory **47**(3), 1212–1215 (2001). https://doi.org/10.1109/18.915688
23. Micciancio, D., Voulgaris, P.: A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. SIAM J. Comput. **42**(3), 1364–1391 (2013). https://doi.org/10.1137/100811970
24. Milnor, J., Husemoller, D.: Symmetric Bilinear Forms. Springer, Heidelberg (1973). ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73
25. Reuland, G.: A Compact Representation of the Voronoi Cell. École Polytechnique Fédérale de Lausanne, January 2018. Master thesis
26. Seysen, M.: A measure for the non-orthogonality of a lattice basis. Combin. Probab. Comput. **8**(3), 281–291 (1999). https://doi.org/10.1017/S0963548399003764
27. Sommer, N., Feder, M., Shalvi, O.: Finding the closest lattice point by iterative slicing. SIAM J. Discrete Math. **23**(2), 715–731 (2009). https://doi.org/10.1137/060676362
28. Vallentin, F.: Sphere coverings, lattices, and tilings (in low dimensions). Ph.D. thesis, Technical University Munich, Germany (2003). http://nbn-resolving.de/urn/resolver.pl?urn:nbn:de:bvb:91-diss2003112600173, 128 p
29. Voronoi, G.: Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Deuxième mémoire. Recherches sur les parallélloèdres primitifs. J. Reine Angew. Math. **134**, 198–287 (1908). https://doi.org/10.1515/crll.1908.134.198