Mathematical Programming (2020) 183:337–358
https://doi.org/10.1007/s10107-019-01463-3

FULL LENGTH PAPER

Series B

On compact representations of Voronoi cells of lattices

Christoph Hunkenschröder[1] · **Gina Reuland**[1] · **Matthias Schymura**[1]

Received: 28 May 2019 / Accepted: 23 December 2019 / Published online: 2 January 2020

Abstract

In a seminal work, Micciancio and Voulgaris (SIAM J Comput 42(3):1364–1391, 2013) 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 · Voronoi cells · Lattices · Zonotopes

Mathematics Subject Classification 11H06 · 52C07 · 68Q25

This work was supported by the Swiss National Science Foundation (SNSF) within the project *Convexity, geometry of numbers, and the complexity of integer programming (No. 163071)*. The paper grew out of the master thesis of the second author [24]; an extended abstract of this work appeared as [16].

✉ Matthias Schymura
matthias.schymura@epfl.ch

Christoph Hunkenschröder
christoph.hunkenschroder@epfl.ch

Gina Reuland
ginareuland@gmail.com

[1] École Polytechnique Fédérale de Lausanne, 1015 Lausanne, Switzerland

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 distance $\|t - z\|$ from t to a lattice point $z \in \Lambda$.

Let us recall the milestones of the algorithmic development regarding both SVP and CVP. For a more detailed overview we refer to Hanrot et al. [15], as well as to the more recent Gaussian Sampling approaches, for example, the one by Aggarwal and Stephens-Davidowitz [1].

In the 1980's, Kannan presented algorithms solving SVP and CVP in running time $n^{\mathcal{O}(n)}$ and polynomial space [17]. Although the constants involved in the running time had been improved, it took roughly fifteen years until a significantly better algorithm was discovered. In 2001, Ajtai et al. [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 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 and Voulgaris [22], 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*. 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 [22] and our notion of compactness we obtain (cf. Corollary 4):

(i) Given a c-compact basis of a lattice $\Lambda \subseteq \mathbb{R}^n$, we can solve the Closest Vector Problem in $(2c+1)^{\mathcal{O}(n)}\,\mathrm{poly}(n)$ time 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 (i) 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 lattices whose Voronoi cell is a zonotope are as compact as possible:

(ii) If the Voronoi cell of Λ is a zonotope, then $c(\Lambda) = 1$. Moreover, a 1-compact basis can be found among the Voronoi relevant vectors.

Furthermore, every lattice of rank at most four has a 1-compact basis (cf. Corollary 3). 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 implicitly formulated in [10,11], and results of Seysen [25] imply that $c(\Lambda) \in n^{\mathcal{O}(\log n)}$. We improve this to a polynomial bound and, on the negative side, we show that $c(\Lambda)$ may grow linearly with the dimension (Sects. 2.1, 2.2):

(iii) Every lattice possesses a basis that is n^2-compact.
(iv) There exists a family of lattices $(\Lambda_n)_{n\geq 5}$ without a $o(n)$-compact basis.

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. Our results regarding the relaxed compactness constant include the following:

(v) For every lattice Λ, we have $\bar{c}(\Lambda) \in \mathcal{O}(n \log n)$.
(vi) 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 and 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.

2 The notion of a *c*-compact basis

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

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

where $\|\cdot\|$ denotes the Euclidean norm. It consists of all points that are at least as close to the origin as 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*, or simply *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 Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and let $c \in \mathbb{N}$. A basis B of Λ is called *c-compact*, if

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

That is, each Voronoi relevant vector is a linear combination of the basis vectors with coefficients bounded by c in absolute value. Moreover, we define

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

as the *compactness constant* of Λ.

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 $K^\star = \{x \in \mathbb{R}^n : x^\intercal y \leq 1 \text{ for all } y \in K\}$ 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 $B^{-\intercal} := (B^{-1})^\intercal$ 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 $(AK)^\star = A^{-\intercal}K^\star$. To keep notation short, the convex hull of a finite point set $S \subseteq \mathbb{R}^n$ will be denoted by $\mathrm{conv}(S) = \{\sum_{s\in S} \alpha_s s \mid \forall s \in S : \alpha_s \in \mathbb{R}_{\geq 0},\ \sum_{s\in S} \alpha_s = 1\}$, and the linear span of S will be denoted by $\mathrm{lin}(S) = \{\sum_{s\in S} \alpha_s s \mid \forall s \in S : \alpha_s \in \mathbb{R}\}$. We refer to Gruber's textbook [14] for details and more information on these concepts.

Lemma 1 *Let $B = \{b_1, \ldots, b_n\}$ 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* $B^{-\mathsf{T}} = \{b_1^\star, \ldots, b_n^\star\}$, *we have*

$$\mathcal{F}_\Lambda \subseteq \left\{x \in \Lambda : |x^\mathsf{T} b_i^\star| \leq c \text{ for all } 1 \leq i \leq n\right\},$$

(iv) $\mathcal{F}_\Lambda \subseteq c\, P_B$, *where* $P_B = \sum_{i=1}^n [-b_i, b_i]$.

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

(i) $\Longleftrightarrow$ (iii): $B = \{b_1, \ldots, b_n\}$ 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 $|\alpha_i| \leq c$, for all $1 \leq i \leq n$. By the definition of the dual basis, we have $\alpha_i = v^\mathsf{T} b_i^\star$, which proves the claim.

(i) $\Longleftrightarrow$ (iv): By definition, $\mathcal{F}_\Lambda \subseteq c\, P_B$ if and only if for every $v \in \mathcal{F}_\Lambda$, there are coefficients $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ such that $v = \sum_{i=1}^n \alpha_i b_i$ and $|\alpha_i| \leq c$. 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 et al. [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 [25] on simultaneous lattice reduction of the primal and dual lattice imply that

$$c(\Lambda) \leq \chi(\Lambda) \in n^{\mathcal{O}(\log n)}. \tag{1}$$

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 $1 \leq i \leq n$, the ith successive minimum is defined as

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

Minkowski's development of his Geometry of Numbers was centered around the study of these 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

$$c(\Lambda) \geq \lambda_n(Q^\star, \Lambda^\star),$$

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 *For a lattice $\Lambda \subseteq \mathbb{R}^n$ with Voronoi cell $\mathcal{V}_\Lambda$ holds $\lambda_1(\mathcal{V}_\Lambda^\star, \Lambda^\star) \leq \frac{2}{\pi} n$. Hence, there exists a dual lattice vector $y^\star \in \Lambda^\star$ such that*

$$\mathcal{V}_\Lambda \subseteq \left\{ x \in \mathbb{R}^n : |x^\mathsf{T} y^\star| \leq \tfrac{2}{\pi} n \right\}.$$

Proof By Minkowski's fundamental theorem (cf. [14, Ch. 22]), we have

$$\lambda_1(\mathcal{V}_\Lambda, \Lambda) \leq 2 \left(\frac{\det(\Lambda)}{\operatorname{vol}(\mathcal{V}_\Lambda)} \right)^{\frac{1}{n}} \quad \text{and} \quad \lambda_1(\mathcal{V}_\Lambda^\star, \Lambda^\star) \leq 2 \left(\frac{\det(\Lambda^\star)}{\operatorname{vol}(\mathcal{V}_\Lambda^\star)} \right)^{\frac{1}{n}}.$$

Moreover, by a result of Kuperberg [18, Cor. 1.6], $\operatorname{vol}(K) \operatorname{vol}(K^\star) \geq \pi^n / n!$, for every centrally symmetric convex body $K \subseteq \mathbb{R}^n$. Therefore,

$$\lambda_1(\mathcal{V}_\Lambda, \Lambda) \lambda_1(\mathcal{V}_\Lambda^\star, \Lambda^\star) \leq 4 \left(\frac{\det(\Lambda) \det(\Lambda^\star)}{\operatorname{vol}(\mathcal{V}_\Lambda) \operatorname{vol}(\mathcal{V}_\Lambda^\star)} \right)^{\frac{1}{n}} \leq 4 \left(\frac{n!}{\pi^n} \right)^{\frac{1}{n}} \leq \frac{4}{\pi} n,$$

since $\det(\Lambda) \det(\Lambda^\star) = 1$ (cf. [19, Ch. 1]). The claimed bound now follows as $\lambda_i(\mathcal{V}_\Lambda, \Lambda) = 2$, for all $1 \leq i \leq n$. □

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 is a basis $D = \{y_1, \ldots, y_n\}$ of $\Lambda^\star$ such that

$$\mathcal{V}_\Lambda \subseteq \left\{ x \in \mathbb{R}^n : |x^\mathsf{T} y_i| \leq \tfrac{1}{2} n^2,\ 1 \leq i \leq n \right\}. \tag{2}$$

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 containment (2) is trivially true, hence let $n \geq 2$. 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 $\mathcal{V}_\Lambda \subseteq \left\{ x \in \mathbb{R}^n : |x^\mathsf{T} y_1| \leq \frac{2n}{\pi} \right\}$. Let $\Lambda' = \Lambda \cap \{x \in \mathbb{R}^n : x^\mathsf{T} y_1 = 0\}$, and observe that the orthogonal projection $\pi : \mathbb{R}^n \to \{x \in \mathbb{R}^n : x^\mathsf{T} y_1 = 0\}$ fulfills $\pi(\Lambda^\star) = (\Lambda')^\star$, where we dualize with respect to the linear span of Λ' (cf. [19, Ch. 1]). By induction hypothesis, there is a basis $D' = \{y_2', \ldots, y_n'\}$ of $(\Lambda')^\star$, such that

$$\mathcal{V}_{\Lambda'} \subseteq \left\{ x \in \mathbb{R}^n : x^\mathsf{T} y_1 = 0 \text{ and } |x^\mathsf{T} y_i'| \leq \tfrac{1}{2}(n-1)^2,\ 2 \leq i \leq n \right\}.$$

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 $2 \leq i \leq n$, and $D = \{y_1, \ldots, y_n\}$ 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 Since 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 $\Lambda \subseteq \mathbb{R}^n$ (compare with (1)).

Let us look at the constant $c(\Lambda)$ from a different angle. A basis of a lattice is particularly nice if each Voronoi relevant vector is a $\{-1, 0, 1\}$-combination of the basis vectors. As not every lattice possesses such a basis (see Proposition 1 below), we relaxed the condition on the coefficients and introduced the lattice parameter $c(\Lambda)$, defined for all lattices. Another way to relax the setting above is not to insist on a basis of Λ, but rather to look for a generating set S such that each Voronoi relevant vector can be written as a $\{-1, 0, 1\}$-combination of the vectors in S. In this setting, we are interested in finding a small set S. Such an S of order $n \log n$ can be retrieved from an n^2-compact basis.

Corollary 1 *For every lattice $\Lambda \subseteq \mathbb{R}^n$ there exists a subset $S \subseteq \Lambda$ of cardinality $\mathcal{O}(n \log n)$ such that*

$$\mathcal{F}_\Lambda \subseteq \left\{ \sum_{s \in S} \sigma_s\, s : \sigma_s \in \{-1, 0, 1\},\ \textit{for } s \in S \right\}.$$

Proof By Theorem 1, there exists a c-compact basis B of Λ with $c \le n^2$. Let $M := \lfloor \log_2 c \rfloor$. Each $0 \le \alpha \le c$ can be written as $\alpha = \sum_{j=0}^{M} 2^j \sigma_j$, for some unique $\sigma_j \in \{0, 1\}$. For each vector $b_i \in B$ and $0 \le j \le M$, we define the vector

$$s_{i,j} := 2^j b_i.$$

This gives $\mathcal{O}(n \log_2(n^2)) = \mathcal{O}(n \log n)$ vectors in total, and clearly every vector $v = \sum_{i=1}^{n} \alpha_i b_i$ with $|\alpha_i| \le c$ can be written as a linear combination of the $s_{i,j}$ using only coefficients in $\{-1, 0, 1\}$. □

Remark 2 With a different method Daniel Dadush (personal communication) proves that the subset S can be chosen to consist of *Voronoi relevant vectors* itself.

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. This requires some technical work; the pure existence of such a family also follows from Proposition 4 (iii) below. However,

based on the understanding of the lattice discussed in this section, we are able 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

$$\Lambda_n(a) = \left\{ z \in \mathbb{Z}^n : \ z_1 \equiv \cdots \equiv z_n \mod a \right\}, \tag{3}$$

whose dual lattice is given by

$$\Lambda_n(a)^\star = \left\{ z \in \tfrac{1}{a}\mathbb{Z}^n : \mathbf{1}^\mathsf{T} z \in \mathbb{Z} \right\}, \tag{4}$$

where $\mathbf{1} = (1, \ldots, 1)^\mathsf{T}$ denotes the all-one vector. The special structure of these lattices allows us to write down the Voronoi relevant vectors explicitly.

Lemma 3 *Let $n \in \mathbb{N}_{\geq 4}$, $a = \lceil n/2 \rceil$, and write $\Lambda_n = \Lambda_n(a)$. Then, a vector $v \in \Lambda_n$ is strictly Voronoi relevant if and only if either $v = \pm\mathbf{1}$, or there exists an index set $\emptyset \neq S \subsetneq \{1, \ldots, n\}$ such that*

$$v_i = \begin{cases} a - \ell & i \in S \\ -\ell & i \notin S \end{cases}, \quad \text{and} \quad \ell \in \left\{ \left\lfloor \frac{a|S|}{n} \right\rfloor, \left\lceil \frac{a|S|}{n} \right\rceil \right\}. \tag{5}$$

Proof Let us first discuss the vectors $\pm\mathbf{1}$. They have squared norm n, and if there is a shorter vector v, it must contain zero coordinates. But due to the definition of Λ_n, all its coordinates are then multiples of a, so it has squared norm at least $a^2 \geq n^2/4 \geq n$ for $n \geq 4$. Hence, $\pm\mathbf{1}$ are shortest vectors of the lattice and therefore always strictly Voronoi relevant. As we are only interested in the strictly Voronoi relevant vectors in this proof, we will omit the word "strictly" henceforth.

Voronoi characterized a 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 (5).

v Voronoi relevant $\Rightarrow$ v of Shape (5) Let $v \neq \pm\mathbf{1}$ be Voronoi relevant. We have $v \in [-a, a]^n$, as $2a\, e_i \in 2\Lambda_n$ otherwise implies that v is not a shortest vector in its co-set $v + 2\Lambda_n$. Let us first assume that there is an index i such that $v_i \in \{0, \pm a\}$. By definition of Λ_n, we have $v_i \equiv v_j \mod a$, for all j, hence $v \in \{0, \pm a\}^n$. If v has at least two non-zero coordinates, let $\widetilde{v}$ arise from v by changing the sign of exactly one of them. Observe that $\widetilde{v}$ is linearly independent from v, has the same length, and is contained in $v + 2\Lambda_n$. This contradicts the assumption that v was Voronoi relevant. If v has only one non-zero entry, say $v_j \neq 0$, then it is of Shape (5). Indeed, we can either take $S = \{j\}$ and $\ell = 0$, or $S = \{1, \ldots, n\} \backslash \{j\}$ and $\ell = \lceil a(n-1)/n \rceil = a$.

This leaves us with the case $v \in [-(a-1), a-1]^n$. Again, by the definition of Λ_n, there is an integer $1 \leq r \leq a - 1$ such that $v \in \{a - r, -r\}^n$. Let k be the number of entries of v that are equal to $a - r$. Note that $1 \leq k \leq n - 1$ as otherwise $v = \pm\mathbf{1}$. For the norm of v, we obtain

$$\|v\|^2 = nr^2 - 2akr + ka^2.$$

Seen as a rational quadratic function in r, it is minimized for $r' = ak/n$. As increasing or decreasing r by 2 corresponds to adding or subtracting $2 \cdot \mathbf{1} \in 2\Lambda_n$ to v, we must have $r \in [r'-1, r'+1]$. If r' is not integral, this corresponds to $r \in \{\lceil ak/n \rceil, \lfloor ak/n \rfloor\}$. If r' is integral, observe that $r = r' \pm 1$ corresponds to two linearly independent vectors in the same co-set and of the same length, hence again $r = r' \in \{\lceil ak/n \rceil, \lfloor ak/n \rfloor\}$, so that v is indeed of Shape (5).

v of Shape (5) $\Rightarrow$ v Voronoi relevant For the other direction, let v be a vector of Shape (5) with index set S and parameter ℓ. Let $u \in v + 2\Lambda_n$ be a shortest vector within the co-set $v + 2\Lambda_n$. We claim that $u = \pm v$, which will prove that v is Voronoi relevant. To this end, recall from above that necessarily $u \in [-a, a]^n$. Moreover, as $u - v \in 2\Lambda_n$, we have $v_i - v_j \equiv u_i - u_j \mod 2a$. Therefore, if there are indices $i \neq j$ such that $v_i = v_j$, then we have $u_i \equiv u_j \mod 2a$. Unless we are in the extreme case $u \in \{0, \pm a\}^n$ [see Case (a)], this even implies $u_i = u_j$ [see Case (b)].

Case (a): We make a second case distinction depending on the number of non-zero entries of u. This number is always either equal to $|S|$ or $n - |S|$.

Note that the case of u having exactly 1 non-zero entry (i.e. $|S| \in \{1, n-1\}$) will be covered by Case (b) below.

If u has at least 3 non-zero entries ($|S| \in \{3, 4, \ldots, n-3\}$), observe that the vector $u' = (u'_1, \ldots, u'_n)^\mathsf{T}$ defined by $u'_i = |u_i| - 2$ is in the same co-set, but also shorter than u, a contradiction.

For the last case, u having two non-zero entries, the vector u' as above is only strictly shorter if n is odd. If n is even however, u and u' will have the same norm. In this particular case, observe that $a|S|/n \in \{1, a-1\}$, hence $\ell = a|S|/n$, as we do not round. But this is a contradiction, as u and v differ by $\mathbf{1} \notin 2\Lambda_n$, that is, they are not in the same co-set.

Case (b): Henceforth, whenever $v_i = v_j$, we have $u_i = u_j$. By possibly switching to $u' = -u$, we can assume that for some $0 \leq r \leq a$, $u_i = a - r$ for $i \in S$ and $u_j = -r$ for $j \notin S$. This is, $u_i = a - r$ whenever $v_i = a - \ell$ and $u_j = -r$ whenever $v_j = -\ell$. For the norm of u, we obtain

$$\|u\|^2 = |S|(a-r)^2 + (n-|S|)r^2 = nr^2 - 2ar|S| + |S|a^2.$$

Seen as a rational quadratic function in r, this term is uniquely minimized for $\hat{r} = a|S|/n$. Observe that there may be two choices for ℓ, $\lfloor \hat{r} \rfloor$, $\lceil \hat{r} \rceil$. It is clear that r also has to be one of these values, as otherwise u is not a shortest vector in its co-set. But observe that the two choices lead to two vectors whose difference is $\mathbf{1} \notin 2\Lambda_n$. As u and v have to be in the same co-set, we have $u = \pm v$, since we may have switched to $-u$ in the beginning. □

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 $c(\Lambda_n) \geq \lceil \frac{n}{4} \rceil$.*

Proof 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 $\mathbf{1}^\mathsf{T} w = 1$, for instance, take $w = e_1$. This implies that each basis of $\Lambda_n^\star$ contains a vector y such that $\mathbf{1}^\mathsf{T} y$ is an odd integer. In particular, using the characterization of Lemma 1, we know that $c\,Q^\star$ has to contain such a y. As $Q^\star$ is

centrally symmetric, assume $\mathbf{1}^\mathsf{T} y \geq 1$. Further, since $\Lambda_n^\star$ is invariant under permutation of the coordinates, assume the entries of y are ordered non-increasingly,

$$y_1 \geq y_2 \geq \cdots \geq y_n. \tag{6}$$

Let us outline our arguments first: we split $\mathbf{1}^\mathsf{T} y$ 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 $v \in \Lambda_n$ whose first k entries are roughly $n/4$, and its last $n - k$ entries are roughly $-n/4$ by using Lemma 3 and choosing $S = \{1, \ldots, k\}$, $\ell = \lfloor ak/n \rfloor = \lfloor a^2/n \rfloor$. We then obtain $v^\mathsf{T} y \approx \frac{n}{4} A - \frac{n}{4} B \geq n/4$ by carefully 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 $y_k = \frac{z}{a}$. We can assume $z > 0$, since otherwise $B \leq 0$ and we are done since $A + B = \mathbf{1}^\mathsf{T} y \geq 1$. Note that we have $A \geq k y_k = z$ and $B \leq (n - k)\frac{z}{a} \leq z$ by (6). 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 $A \geq \max\{B + 1, 1\}$.

Using this inequality and carefully evaluating $v^\mathsf{T} y = (a - \ell)A - \ell B$ for the four cases $n \mod 4$, the claim follows.

Recall that we construct the Voronoi relevant vector v by choosing $k = a = \lceil n/2 \rceil$, $S = \{1, \ldots, k\}$, $\ell = \lfloor ak/n \rfloor = \lfloor a^2/n \rfloor$, and applying Lemma 3.

We obtain $v^\mathsf{T} y = (a - \ell)A - \ell B$, and are ready to distinguish the four cases $n \mod 4$.

1. $n = 4m$. Hence, we have $a = k = 2m$, and $\ell = m$. Thus,

$$v^\mathsf{T} y = (a - \ell)A - \ell B = m(A - B) \geq m = n/4.$$

2. $n = 4m + 1$. Hence, we have $a = k = 2m + 1$, and $\ell = m$. Thus,

$$v^\mathsf{T} y = (a - \ell)A - \ell B = m(A - B) + A \geq m + 1 \geq n/4.$$

3. $n = 4m + 2$. Hence, we have $a = k = 2m + 1$, and $\ell = m$. Thus,

$$v^\mathsf{T} y = (a - \ell)A - \ell B = m(A - B) + A \geq m + 1 \geq n/4.$$

4. $n = 4m + 3$. Hence, we have $a = k = 2m + 2$, and $\ell = m + 1$. Thus,

$$v^\mathsf{T} y = (a - \ell)A - \ell B = (m + 1)(A - B) \geq m + 1 \geq n/4.$$

As the constant c is integral, the claim follows. □

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 constitute the first reduction domain in Voronoi's reduction theory (see [26,27]). 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 $b_i^\mathsf{T} b_j \leq 0$, 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 $v = \sum_{i \in S} b_i$.

Let us compare lattices of Voronoi's first kind with lattices possessing a compact basis.

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 $D_n = \{x \in \mathbb{Z}^n : \mathbf{1}^\mathsf{T} x \in 2\mathbb{Z}\}$ *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]), so part (i) applies.

(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. One can easily verify that 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. Observing that the vectors $2e_i \pm 2e_j$ are in $2D_n$ for all i, j, a vector v that is the unique (up to sign) shortest vector in the co-set $v + 2\Lambda$, must be 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 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]). However, not every generic lattice is zonotopal. For instance, a perturbation of the E_8 root lattice gives a generic non-zonotopal lattice (cf. [13, Sect. 4]).

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 [26, Ch. 2] and [13]). In the following, we prove that every zonotopal lattice possesses a compact basis, thus extending Proposition 1 (i) significantly.

Our proof relies on the beautiful work of Erdahl [12] who unraveled an intimate relationship between zonotopal lattices and so-called dicings. A *dicing* $\mathfrak{D}$ in $\mathbb{R}^n$ is an arrangement of hyperplanes consisting of at least n families of infinitely many equally-spaced hyperplanes with the following properties:

(i) There are n families with linearly independent normal vectors.
(ii) Every vertex of $\mathfrak{D}$ is contained in a hyperplane of each family.

The interesting cases are those with more than n families of hyperplanes.

It turns out that the vertex set of a dicing forms a lattice, denoted by $\Lambda(\mathfrak{D})$. Indeed, the vertex set induced by the n linearly independent families forms a lattice, and because of property (ii) no additional vertices are introduced by the remaining families. A basis of the lattice $\Lambda(\mathfrak{D})$ may be obtained from taking the inverse of the matrix whose rows are n linearly independent normal vectors appropriately scaled [they exist by property (i)].

Erdahl [12, Thm. 3.1] shows that a dicing $\mathfrak{D}$ can be represented by 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 $\mathfrak{D}$ 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 $d_i^{\mathsf{T}} e_j \in \{0, \pm 1\}$.

For clarity we denote the dicing by $\mathfrak{D} = \mathfrak{D}(D, E)$.

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

Proof We start by reviewing the *Delaunay tiling* of a 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 $B_c(R) \cap \Lambda$, where $B_c(R)$ is an empty sphere. 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 $d_i^{\mathsf{T}} e_j = \delta_{ij}$, with δ_{ij} being the Kronecker delta. Moreover, the set $B = \{e_1, \ldots, e_n\}$ is a basis of $\{x \in \mathbb{R}^n : d_i^{\mathsf{T}} x \in \mathbb{Z}, 1 \leq i \leq n\}$, 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 $d_i^{\mathsf{T}} v \in \{0, \pm 1\}$. In view of Lemma 1 (iii), this means that B is a compact basis of Λ consisting of Voronoi relevant vectors, as desired. □

2.4 Compact bases in small dimensions

We have seen in Proposition 1 that every lattice of rank at most three has a compact basis, and that there are five-dimensional lattices without compact bases. In the sequel

we complete the picture and show that every four-dimensional lattice admits a compact basis as well.

Our argument uses tools from the theory of parallelotopes which requires to set up the compactness constant in this more general framework. For details and background on the following definitions and statements on parallelotopes we refer to [14, §32]. A *parallelotope* (also called parallelohedron) is a convex polytope $P \subseteq \mathbb{R}^n$ that admits a facet-to-facet tiling of $\mathbb{R}^n$ by translations. Voronoi cells of lattices are prime examples of parallelotopes. Every parallelotope is centrally symmetric, and we may assume that its center of symmetry is at the origin. The set of translation vectors that constitute the facet-to-facet tiling by copies of P is in fact a lattice, and we denote it by $\Lambda(P)$. Every facet F of P corresponds to a lattice vector $x \in \Lambda(P)$ such that $P \cap (P + x) = F$. Such a lattice vector is called a *facet vector*. More generally, a lattice vector $x \in \Lambda(P)$ such that $P \cap (P + x)$ is a face of both P and $P + x$ is called a *standard vector* of P.

For Voronoi cells the facet vectors and the standard vectors are exactly the strictly and weakly Voronoi relevant vectors, respectively. Therefore, we can extend our notation from the previous sections from Voronoi cells and lattices, to general parallelotopes: We write $\mathcal{F}_P$ and $\mathcal{C}_P$ for the set of facet vectors and standard vectors of P, respectively, and $c(P)$ and $\chi(P)$ for the corresponding compactness constants. For example, $\chi(P)$ is the minimal $\chi > 0$ such that there is a basis $B = \{b_1, \ldots, b_n\}$ of $\Lambda(P)$ with the property that every standard vector $x \in \mathcal{C}_P$ can be written as $x = \sum_{i=1}^{n} \gamma_i b_i$, for some $|\gamma_i| \leq \chi$.

With this notation we prove the crucial fact, that if a parallelotope Q decomposes into the Minkowski sum of another parallelotope P and a (possibly lower-dimensional) zonotope Z, then $\chi(Q) \leq \chi(P)$. We write $Z(U) = \sum_{i=1}^{r} [-u_i, u_i]$ for the zonotope spanned by the set of vectors $U = \{u_1, \ldots, u_r\}$.

Proposition 2 *Let $Q \subseteq \mathbb{R}^n$ be a parallelotope that admits a decomposition $Q = P + Z(U)$, for some parallelotope P, and a finite set of vectors $U \subseteq \mathbb{R}^n$. Then, there is a linear map $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ with $\varphi(\Lambda(P)) = \Lambda(Q)$ satisfying*

(i) *For $x \in \mathcal{C}_Q$, we have $\varphi^{-1}(x) \in \mathcal{C}_P$.*
(ii) *For $x \in \mathcal{F}_P$, we have $\varphi(x) \in \mathcal{F}_Q$.*

In particular, $\chi(Q) \leq \chi(P)$.

Proof First note that if $P + Z(U)$ is a parallelotope, then every vector $u \in U$ is a *free* vector for P, that is, $P + [-u, u]$ is a parallelotope as well (cf. [9]). We thus get a chain of parallelotopes $P = P_0 \subseteq P_1 \subseteq \ldots \subseteq P_r = Q$, where $P_i = P_{i-1} + [-u_i, u_i]$, for $1 \leq i \leq r$, and $U = \{u_1, \ldots, u_r\}$. By induction on r it thus suffices to consider the case $r = 1$.

Hence, let $Q = P + [-u, u]$, for some non-zero vector $u \in \mathbb{R}^n$. Dutour Sikirić et al. [9, Lem. 1 & Lem. 3] give a characterization of the standard vectors of Q in terms of those of P: First, there is a dual lattice vector $e_u \in \Lambda(P)^\star$ such that $\Lambda(Q) = A_u \Lambda(P)$, where $A_u x = x + 2(e_u^\mathsf{T} x)u$, for $x \in \mathbb{R}^n$. Then, $z = A_u w \in \Lambda(Q)$ is a standard vector of Q if and only if w is a standard vector of P, and $e_u^\mathsf{T} w \in \{0, \pm 1\}$.

This implies that $\varphi(x) = A_u x$ is a bijection between the lattices $\Lambda(P)$ and $\Lambda(Q)$ satisfying (i). Moreover, the proof of [9, Lem. 1] reveals that A_u, and thus φ, sends facet

vectors to facet vectors, hence $ii)$ holds as well. For $r \geq 2$, we define φ inductively by setting $\varphi(x) = A_{u_r} \cdot \ldots \cdot A_{u_1} x$.

Finally we show that $\chi(Q) \leq \chi(P)$. As just observed, any basis B of $\Lambda(P)$ is sent to a basis $\varphi(B)$ of $\Lambda(Q)$. Moreover, a standard vector $y = \sum_{i=1}^{n} \alpha_i \varphi(b_i) \in \mathcal{C}_Q$ represented in the basis $\varphi(B)$ corresponds to a standard vector $\varphi^{-1}(y) = \sum_{i=1}^{n} \alpha_i b_i \in \mathcal{C}_P$ using the same coefficients when represented in the basis B. Thus, if every vector in $\mathcal{C}_P$ can be represented in B with coefficients bounded by $\chi(P)$, the same holds for all vectors in $\mathcal{C}_Q$ with respect to $\varphi(B)$. □

As a consequence, we get that zonotopal parallelotopes Z allow for a compact representation even of the set $\mathcal{C}_Z$ which strengthens Theorem 3. In particular, every three-dimensional parallelotope has this property (cf. [14, §32.2]).

Corollary 2 *Let Z be a parallelotope that is a zonotope. Then $\chi(Z) = 1$.*

Proof There is a set of vectors $U' = \{u_1, \ldots, u_m\}$ such that $Z = Z(U')$. We may assume that $u_1, \ldots, u_n$ are linearly independent, and we write $P = [-u_1, u_1] + \cdots + [-u_n, u_n]$. Then, $Z = P + Z(U)$, for $U = U' \backslash \{u_1, \ldots, u_n\}$, and since P is a parallelepiped, it is actually a parallelotope.

Thus, Proposition 2 implies that $\chi(Z) \leq \chi(P)$ and it suffices to show that $\chi(P) = 1$ for every parallelepiped P. The standard vectors of P are exactly those $x \in \Lambda(P) \backslash \{0\}$ such that $P \cap (x + P) \neq \emptyset$. Writing $\pm f_1, \ldots, \pm f_n$ for the n pairs of facet vectors of P, we find that $\{f_1, \ldots, f_n\}$ is a basis of $\Lambda(P)$ in which every standard vector admits a $\{0, \pm 1\}$-representation. □

We now focus again on parallelotopes that are Voronoi cells but work in the more convenient language of quadratic forms. A famous conjecture of Voronoi states that every parallelotope is an affine image of a Voronoi cell of a lattice (cf. [14, §32]). As long as this is not settled we need to make the distinction.

Let $q : \mathbb{R}^n \to \mathbb{R}$ be a positive definite quadratic form defined by $q(x) = x^\mathsf{T} A^\mathsf{T} A x$, for some invertible matrix $A \in \mathbb{R}^{n \times n}$. We associate the lattice $\Lambda = A\mathbb{Z}^n$ to q. Analogously to the lattice case, the Voronoi cell of q is defined as

$$\mathcal{V}_q = \left\{ x \in \mathbb{R}^n : q(x) \leq q(x - z) \text{ for all } z \in \mathbb{Z}^n \right\}.$$

This is a linear image of the Voronoi cell of Λ and thus a parallelotope. For the sake of brevity we use the shorter notations $\mathcal{F}_q = \mathcal{F}_{\mathcal{V}_q}$, $\mathcal{C}_q = \mathcal{C}_{\mathcal{V}_q}$, $c(q) = c(\mathcal{V}_q)$, and $\chi(q) = \chi(\mathcal{V}_q)$. The exact correspondences between the various notions in the languages of lattices and quadratic forms are as follows.

Lemma 4 *Let $q : \mathbb{R}^n \to \mathbb{R}$ be a positive definite quadratic form defined by $q(x) = x^\mathsf{T} A^\mathsf{T} A x$, for some invertible matrix $A \in \mathbb{R}^{n \times n}$. Moreover, write $\Lambda = A\mathbb{Z}^n$ for the lattice generated by A. Then,*

(i) $\mathcal{V}_\Lambda = A\,\mathcal{V}_q$ *and* $\mathcal{F}_\Lambda = A\,\mathcal{F}_q$,
(ii) $c(q) = c(\Lambda)$ *and* $\chi(q) = \chi(\Lambda)$.

Proof For (i), observe that

$$\begin{aligned}\mathcal{V}_q &= \left\{x \in \mathbb{R}^n : \|Ax\|^2 \le \|A(x-z)\|^2 \text{ for all } z \in \mathbb{Z}^n\right\} \\ &= \left\{A^{-1}y \in \mathbb{R}^n : \|y\|^2 \le \|y - Az\|^2 \text{ for all } z \in \mathbb{Z}^n\right\} = A^{-1}\mathcal{V}_\Lambda.\end{aligned}$$

For the second identity, notice that $x \in \mathcal{F}_q$ if and only if $\mathcal{V}_q \cap (\mathcal{V}_q + x)$ is a facet of $\mathcal{V}_q$, which holds if and only if $A\mathcal{V}_q \cap (A\mathcal{V}_q + Ax)$ is a facet of $A\mathcal{V}_q = \mathcal{V}_\Lambda$. Part (ii) is a direct consequence of these observations. □

The lattice $D_4 = \{z \in \mathbb{Z}^4 : z_1 + \cdots + z_4 \in 2\mathbb{Z}\}$ plays a crucial role in representing 4-dimensional lattices whose Voronoi cell is not a zonotope, and thus deserves a detailed study.

Lemma 5 *Let $y \in \mathcal{C}_{D_4} \backslash \mathcal{F}_{D_4}$. Then there is a basis B of D_4 such that*

$$\mathcal{C}_{D_4} \backslash \{\pm y\} \subseteq \{Bz : \|z\|_\infty \le 1\}.$$

Proof We start by characterizing the sets $\mathcal{F}_{D_4}$ and $\mathcal{C}_{D_4}$. Since $\pm 2e_i \pm 2e_j \in 2D_4 \subseteq 2\mathbb{Z}^4$ for $1 \le i < j \le 4$, it follows that $S = \{z \in \{0, \pm 1\}^4 : \|z\|^2 \in \{2, 4\}\}$ contains all vectors $v \ne 0$ that are shortest in their respective co-set $v + 2D_4$. In fact, due to parity of the coefficients, we have $S = \mathcal{C}_{D_4}$. In the proof of Proposition 1, we saw that $\mathcal{F}_{D_4} \subseteq \{z \in D_4 : \|z\|^2 = 2\}$. For parity reasons of $z \in \mathcal{F}_{D_4}$, the vectors z and $-z$ are the unique shortest vectors in $z + 2D_4$, hence we actually have $\mathcal{F}_{D_4} = \{z \in D_4 : \|z\|^2 = 2\}$.

Now, let $y \in \mathcal{C}_{D_4} \backslash \mathcal{F}_{D_4}$ and observe that $D_4^\star = \mathbb{Z}^4 \cup (\frac{1}{2}\mathbf{1} + \mathbb{Z}^4)$. Then

$$\left\{x \in \mathbb{R}^4 : |e_i^\mathsf{T} x| \le 1, 1 \le i \le 4\right\} \cap \left\{x \in \mathbb{R}^4 : |y^\mathsf{T} x| \le 2\right\}$$

is a facet-description of $Q := \operatorname{conv}\{\mathcal{C}_{D_4} \backslash \{\pm y\}\}$. The inequality $|y^\mathsf{T} x| \le 2$ arises since the vectors $y_i e_i + y_j e_j$, $1 \le i < j \le 4$ are contained in $\mathcal{C}_{D_4} \backslash \{\pm y\}$. Taking polars, we obtain that

$$Q^\star = \operatorname{conv}\left(\{\pm e_i : i = 1, \ldots, 4\} \cup \{\pm \tfrac{1}{2} y\}\right),$$

and we see that $Q^\star$ contains the dual lattice basis $B^{-\mathsf{T}} = \{\frac{1}{2}y, e_1, e_2, e_3\}$. Hence, in the spirit of Lemma 1, every vector in $\mathcal{C}_{D_4} \backslash \{\pm y\}$ is represented with coefficients in $\{\pm 1, 0\}$ in the corresponding primal basis B. □

Observe that Lemma 5 is best possible in the sense that $\chi(D_4) = 2$.[1] In order to see this, $\operatorname{conv}(\mathcal{C}_{D_4})^\star$ is the standard crosspolytope, which does not contain a basis of $D_4^\star$ as any such basis has to contain a vector in $\frac{1}{2}\mathbf{1} + \mathbb{Z}^4$. However, after dilating by 2, we find the basis $\{\frac{1}{2}\mathbf{1}, e_2, e_3, e_4\}$ of $D_4^\star$ (cf. Lemma 1).

We now arrive at the desired compactness of four-dimensional lattices.

[1] Engel et al. [11] claim that they computed $\chi(D_4) = 1$, which turns out to be wrong.

Table 1 Compactness of lattices in small dimensions

Dimension of Λ	Compactness result	Reference
$n \leq 3$	$c(\Lambda) = \chi(\Lambda) = 1$	Proposition 1 and Corollary 2
$n = 4$	$c(\Lambda) = 1$, but $\chi(D_4) = 2$	Corollary 3
$n \geq 5$	$c(\Lambda_n) \geq \lceil \frac{n}{4} \rceil$	Theorem 2

Corollary 3 *Every lattice of rank at most four has a compact basis.*

Proof We have seen in Proposition 1 (ii), that every lattice of rank at most three has a compact basis. Thus, let $\Lambda = A\mathbb{Z}^4$ be a full-dimensional lattice, and let $q(x) = x^\mathsf{T} A^\mathsf{T} A x$ be the corresponding quadratic form. In the case that $\mathcal{V}_q$ is a zonotope, we use Lemma 4 to get that $\mathcal{V}_\Lambda = A\,\mathcal{V}_q$ is a zonotope as well, and thus Theorem 3 implies that $c(\Lambda) = 1$.

If $\mathcal{V}_q$ is not a zonotope, then Voronoi's reduction theory as applied in Vallentin's thesis [26, Ch. 3] shows the following: We can write $\mathcal{V}_q = \mathcal{V}_p + Z(U)$, for some positive definite quadratic form p and a set of vectors $U \subseteq \mathbb{R}^4$. Moreover, p is such that $\mathcal{V}_p$ is combinatorially equivalent to the 24-cell. Up to isometries and scalings, the only lattice whose Voronoi cell is combinatorially equivalent to the 24-cell is the root lattice D_4, defined in Proposition 1. This is due to the fact that D_4 is what is called a *rigid* lattice. Therefore, any lattice corresponding to p agrees with D_4 up to isometries and scalings.

By Lemmas 4 and 5, this means that for every vector $y \in \mathcal{C}_p \backslash \mathcal{F}_p$, we can find a basis B of $\Lambda_p := \Lambda(\mathcal{V}_p)$ such that every standard vector of $\mathcal{V}_p$ apart from $\pm y$ can be represented with coefficients in $\{\pm 1, 0\}$. By the first part of Proposition 2, there is a linear map φ such that $\varphi(\Lambda_p) = \Lambda_q := \Lambda(\mathcal{V}_q)$, and $\varphi^{-1}(\mathcal{F}_q) =: \mathcal{C}' \subseteq \mathcal{C}_p$. By the second part of Proposition 2, we have $\mathcal{F}_p \subseteq \mathcal{C}'$. Since $A\mathcal{V}_q$ is a Voronoi cell, we have $|\mathcal{C}'| = |\mathcal{F}_q| \leq 2(2^4 - 1) = 30$, whereas $|\mathcal{C}_p| = |\mathcal{C}_{D_4}| = 40$ (see the proof of Lemma 5). Hence we can choose $y \in \mathcal{C}_p \backslash \mathcal{C}'$, and find a basis B of $\mathcal{V}_p$ so that all vectors in $\mathcal{C}'$ are represented with coefficients in $\{0, \pm 1\}$. This implies that all vectors in $\mathcal{F}_q$ have coefficients in $\{0, \pm 1\}$ when represented in the basis $\varphi(B)$ of $\mathcal{V}_q$. Thus, the lattice Λ has a compact basis as $c(q) = c(\Lambda)$. □

We summarize the results of this section in Table 1.

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. This is due to the fact that, given a basis, membership to a lattice can be checked in polynomial time. Thus, in case that the relaxation improves the compactness of the presentation, this additional check is faster than iterating over the larger set corresponding to a $c(\Lambda)$-compact basis.

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

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

Moreover, we define

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

as the *relaxed compactness constant* of Λ.

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 relaxed compactness constant and $c(\Lambda)$ are related as follows.

Proposition 3 *For every lattice* Λ *in* $\mathbb{R}^n$, $n \geq 2$, *we have*

$$\bar{c}(\Lambda) = \lambda_n(Q^\star, \Lambda^\star) \quad \textit{and} \quad \bar{c}(\Lambda) \leq c(\Lambda) \leq \frac{n}{2}\,\bar{c}(\Lambda),$$

where $Q = \operatorname{conv}(\mathcal{F}_\Lambda)$ *as before.*

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.

In order to prove that $c(\Lambda) \leq \frac{n}{2}\,\bar{c}(\Lambda)$, we let $v_1, \ldots, v_n \in (\bar{c}(\Lambda) \cdot Q^\star) \cap \Lambda^\star$ be linearly independent, and for $1 \leq k \leq n$, we consider the crosspolytope $C_k = \operatorname{conv}\{\pm v_1, \ldots, \pm v_k\}$. We show by induction that there are vectors $u_1, \ldots, u_n \in \Lambda^\star$ such that (a) $\{u_1, \ldots, u_k\}$ is a basis of the lattice $\Lambda^\star \cap \operatorname{lin}\{v_1, \ldots, v_k\}$, and (b) $u_k \in \max\{\frac{k}{2}, 1\} \cdot C_k$, for every $1 \leq k \leq n$. This then implies that $\{u_1, \ldots, u_n\}$ is a basis of $\Lambda^\star$ contained in $\frac{n}{2}\,C_n \subseteq \frac{n}{2}\,\bar{c}(\Lambda)\,Q^\star$. Hence, $c(\Lambda) \leq \frac{n}{2}\,\bar{c}(\Lambda)$, as desired.

First, at least one of the vectors $v_1, \ldots, v_n$ must be primitive, say v_1. Then, setting $u_1 = v_1$ gets the induction started. Now, let us assume that we found $u_1, \ldots, u_{k-1}$ satisfying (a) and (b). Let $y \in (\Lambda^\star \cap \operatorname{lin}\{v_1, \ldots, v_k\})^\star$ be a primitive vector orthogonal to $\operatorname{lin}\{u_1, \ldots, u_{k-1}\}$ and such that $y^\intercal v_k \neq 0$. If $|y^\intercal v_k| = 1$, then $u_k = v_k \in C_k$ complements $\{u_1, \ldots, u_{k-1}\}$ to a basis of $\Lambda^\star \cap \operatorname{lin}\{v_1, \ldots, v_k\}$. So, we may assume that $|y^\intercal v_k| \geq 2$. Every translate of $\frac{k-1}{2}\,C_{k-1}$ within $\operatorname{lin}\{v_1, \ldots, v_{k-1}\}$ contains a point of $\Lambda^\star$. In particular, there is a vector $u_k \in \Lambda^\star$ contained in $\frac{1}{y^\intercal v_k}\,v_k + \frac{k-1}{2}\,C_{k-1}$. By construction, u_k complements $\{u_1, \ldots, u_{k-1}\}$ to a basis of $\Lambda^\star \cap \operatorname{lin}\{v_1, \ldots, v_k\}$, and since $|\frac{1}{y^\intercal v_k}| \leq \frac{1}{2}$, we get that $u_k \in \frac{1}{2}\,C_k + \frac{k-1}{2}\,C_{k-1} \subseteq \frac{k}{2}\,C_k$. □

The relaxation to representing $\mathcal{F}_\Lambda$ by generating sets rather than by lattice bases may reduce the respective compactness constant drastically. In fact, the quadratic upper bound in Theorem 1 improves to $\mathcal{O}(n \log n)$. However, there is still a class of lattices that shows 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 $n/2$ 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 (3). 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

$$\bar{c}(\Lambda) = \lambda_n(Q^\star, \Lambda^\star) = \lambda_1(Q, \Lambda) \cdot \lambda_n(Q^\star, \Lambda^\star) \leq \gamma\, n \log n. \tag{7}$$

(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.

First of all, they are clearly linearly independent, and the description (4) shows that all these vectors belong to $\Lambda_n^\star$. Now, recall that $Q^\star = \{y \in \mathbb{R}^n : y^\mathsf{T} v \leq 1 \text{ for all } v \in \mathcal{F}_{\Lambda_n}\}$. By Lemma 3, a Voronoi relevant vector v of Λ_n either equals $\pm\mathbf{1}$ or is contained in $v \in \{a-\ell, -\ell\}^n$, for some suitable $\ell \in \mathbb{N}$. Consider first the vectors y_i, for $1 \leq i \leq n-1$. We have $\mathbf{1}^\mathsf{T} y_i = 0$, and for any $v \in \{a-\ell, -\ell\}^n$ holds $v^\mathsf{T} y_i = \frac{1}{a}(v_i - v_n)$ which equals 0, if $v_i = v_n$, and it equals ± 1, if $v_i \neq v_n$. Thus, in fact $y_1, \ldots, y_{n-1} \in Q^\star$.

Regarding the remaining vector y_n, we observe that $\mathbf{1}^\mathsf{T} y_n = 2$, independently of the parity of the dimension n. Thus, let $v \in \{a-\ell, -\ell\}^n$, and note that $\ell \in \{\lfloor \frac{ak}{n} \rfloor, \lceil \frac{ak}{n} \rceil\}$, where $k = |\{i : v_i = a - \ell\}|$.

Since $-\ell \leq a$ and $a - \ell \leq a$, we have

$$\begin{aligned} y_n^\mathsf{T} v &\leq \tfrac{1}{a}\left(k(a-\ell) - (n-k)\ell + a\right) = \tfrac{1}{a}\left(ka - n\ell + a\right) \\ &\leq \tfrac{1}{a}\left(ka - n(\tfrac{ak}{n} - 1) + a\right) = \frac{n+a}{a} \leq 3, \end{aligned}$$

and similarly $y_n^\mathsf{T} v \geq -3$. Hence, $y_n \in 3\,Q^\star$, finishing the proof.

(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 $v^\mathsf{T} x \leq \frac{1}{2}\|v\|^2$, as well as a facet of $Q^\star$ via the inequality $v^\mathsf{T} x \leq 1$ (this indeed defines a facet, as a vertex v of Q always induces a corresponding facet of the polar $Q^\star$). 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 and Thompson (see [23, 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 (7) is linear in n, we conjecture the following:

Conjecture 1 The compactness constants are linearly bounded, that is

$$\bar{c}(\Lambda) \in \mathcal{O}(n) \quad \text{and also} \quad c(\Lambda) \in \mathcal{O}(n),$$

for every lattice $\Lambda \subseteq \mathbb{R}^n$.

4 Algorithmic point of view

When it comes to computing a $c(\Lambda)$-compact basis for Λ, not much is known. Lemma 1 suggests to take the polar of $\text{conv}(\mathcal{F}_\Lambda)$, 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. Even if we are only interested in an $(n \cdot c(\Lambda))$-compact basis, it is not clear how to benefit from the allowed slack.

In the following, we rather discuss how to incorporate an already known c-compact basis into the algorithm of Micciancio and Voulgaris [22].

The Micciancio–Voulgaris algorithm

The 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. As a c-compact basis already grants a superset of $\mathcal{F}_\Lambda$, we do not recall the details of this first part.

Once the Voronoi cell $\mathcal{V}_\Lambda$ is computed, a vector $p \in \Lambda$ is closest to t if and only if $t - p \in \mathcal{V}_\Lambda$. Bearing this in mind, the idea is to iteratively subtract lattice vectors from t until the condition holds.

But why do we only need $2^{\mathcal{O}(n)}$ iterations? Let us assume for now that t is already rather close to 0, say $t \in 2\,\mathcal{V}_\Lambda$. Let p be a Voronoi relevant vector whose induced facet-defining inequality is violated by t, this means $p^\intercal t > \frac{1}{2}\|p\|^2$. Micciancio and Voulgaris show that $t - p$ is still contained in $2\,\mathcal{V}_\Lambda$, and is strictly shorter than t. Hence, for going from $t \in 2\,\mathcal{V}_\Lambda$ to some $t' = t - w \in \mathcal{V}_\Lambda$, for $w \in \Lambda$, the number of iterations we need is bounded by the number of level sets of the norm function that have a point in $2\,\mathcal{V}_\Lambda \cap (t + \Lambda)$. This number turns out to be at most 2^n.

If t is further away, that is $t \notin 2\,\mathcal{V}_\Lambda$, let k be the smallest integer such that $t \in 2^k \mathcal{V}_\Lambda$. Then, we can apply the above method to the lattice $\Lambda' = 2^{k-1}\Lambda$, and find $w \in \Lambda' \subseteq \Lambda$ such that $t - w \in \mathcal{V}_{\Lambda'} = 2^{k-1}\mathcal{V}_\Lambda$. Doing this recursively yields that after $2^n k$ iterations, we moved t into $\mathcal{V}_\Lambda$. Note that k is polynomial in the input size. More sophisticated arguments allow to limit k in terms of n only, or to decrease the number of iterations to weakly polynomial, as presented in [5].

Corollary 4 *Assume 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 $\mathcal{O}((2c+1)^n\, 2^n\, \mathrm{poly}(n))$ and space polynomial in the input size.*

Proof Theorem 4.2 and Remark 4.4 in [22] state that a closest vector can be found in time $\mathcal{O}(|V| \cdot 2^n\, \mathrm{poly}(n))$, 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 [22, 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 we are allowed to use the information we gathered before to speed up the process of finding a closest vector. This is motivated by the fact that in practice, we might have to compute the closest vector for several target vectors, but always on the same lattice. Hence, we happily spend more time for preprocessing, when we are able to vastly benefit from the additional information.

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

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

The fact that every zonotopal lattice has a compact basis is especially interesting. McCormick, Peis, Scheidweiler & Vallentin can solve the Closest Vector Problem in polynomial time on a zonotopal lattice, provided it is given in a certain format.[2] Another related result is due to McKilliam et al. [20], who provide a polynomial time algorithm for lattices of Voronoi's first kind, provided an obtuse superbasis is known. One could wonder whether our representation also allows for solving CVPP faster (measuring only the time after the preprocessing). However, McKilliam et al. use additional combinatorial properties of an obtuse superbasis that are in general not even fulfilled for a 1-compact basis. In fact, Micciancio [21] showed that if CVPP can be solved in polynomial time for arbitrary lattices, then NP $\subseteq$ P/poly and the polynomial hierarchy collapses.

Acknowledgements 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 $\mathcal{O}(n^2 \log n)$. We are grateful to the referees for their valuable suggestions, questions, and comments.

References

1. Aggarwal, D., Stephens-Davidowitz, N.: Just take the average! An embarrassingly simple 2^n-time algorithm for SVP (and CVP). In: 1st Symposium on Simplicity in Algorithms (SOSA 2018), Ope-

[2] At the time of writing there is no preprint available (personal communication with Frank Vallentin).

nAccess Series in Informatics (OASIcs), vol. 61, pp. 12:1–12:19. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik (2018)
2. Ajtai, M., Kumar, R., Sivakumar, D.: A sieve algorithm for the shortest lattice vector problem. In: Proceedings of Thirty-Third annual ACM Symposium on Theory of Computing, pp. 601–610. ACM (2001)
3. Ajtai, M., Kumar, R., Sivakumar, D.: Sampling short lattice vectors and the closest lattice vector problem. In: Proceedings of 17th IEEE Annual Conference on Computational Complexity, pp. 53–57. IEEE (2002)
4. Banaszczyk, W.: Inequalities for convex bodies and polar reciprocal lattices in $\mathbf{R}^n$. II. Application of K-convexity. Discrete Comput. Geom. **16**(3), 305–311 (1996)
5. Bonifas, N., Dadush, D.: Short paths on the Voronoi graph and closest vector problem with preprocessing. In: Proceedings of Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 295–314. SIAM, Philadelphia (2015)
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)
7. Conway, J.H., Sloane, N.J.A.: Low-dimensional lattices. VI. Voronoĭ reduction of three-dimensional lattices. Proc. R. Soc. Lond. Ser. A **436**(1896), 55–68 (1992)
8. Conway, J.H., Sloane, N.J.A.: Sphere Packings, Lattices and Groups. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, 3rd edn. Springer, New York (1999)
9. Dutour Sikirić, M., Grishukhin, V., Magazinov, A.: On the sum of a parallelotope and a zonotope. Eur. J. Comb. **42**, 49–73 (2014)
10. Engel, P.: Mathematical problems in modern crystallography. Comput. Math. Appl. **16**(5–8), 425–436 (1988)
11. Engel, P., Michel, L., Senechal, M.: New geometric invariants for Euclidean lattices. In: Réseaux euclidiens, designs sphériques et formes modulaires. Monographs of L'Enseignement Mathématique, vol. 37, pp. 268–272. Enseignement Mathématique, Geneva (2001)
12. Erdahl, R.M.: Zonotopes, dicings, and Voronoi's conjecture on parallelohedra. Eur. J. Comb. **20**(6), 527–549 (1999)
13. Erdahl, R.M., Ryshkov, S.S.: On lattice dicing. Eur. J. Comb. **15**(5), 459–481 (1994)
14. Gruber, P.M.: Convex and Discrete Geometry. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 336. Springer, Berlin (2007)
15. Hanrot, G., Pujol, X., Stehlé, D.: Algorithms for the shortest and closest lattice vector problems. In: Coding and Cryptology. Lecture Notes in Computer Science, vol. 6639, pp. 159–190. Springer, Heidelberg (2011). Corrected version at http://perso.ens-lyon.fr/damien.stehle/downloads/SVPCVP.pdf
16. Hunkenschröder, C., Reuland, G., Schymura, M.: On compact representations of Voronoi cells of lattices. In: Proceedings of 20th Conference on Integer Programming and Combinatorial Optimization (IPCO). Lecture Notes in Computer Science, vol. 11480, pp. 261–274. Springer, Cham (2019)
17. Kannan, R.: Minkowski's convex body theorem and integer programming. Math. Oper. Res. **12**(3), 415–440 (1987)
18. Kuperberg, G.: From the Mahler conjecture to Gauss linking integrals. Geom. Funct. Anal. **18**(3), 870–892 (2008)
19. Martinet, J.: Perfect Lattices in Euclidean Spaces. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 327. Springer, Berlin (2003)
20. 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)
21. Micciancio, D.: The hardness of the closest vector problem with preprocessing. IEEE Trans. Inf. Theory **47**(3), 1212–1215 (2001)
22. 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)
23. Milnor, J., Husemoller, D.: Symmetric Bilinear Forms. Springer, New York (1973)
24. Reuland, G.: A Compact Representation of the Voronoi Cell. École Polytechnique Fédérale de Lausanne (January 2018). Master Thesis
25. Seysen, M.: A measure for the non-orthogonality of a lattice basis. Combin. Probab. Comput. **8**(3), 281–291 (1999)

26. Vallentin, F.: Sphere coverings, lattices, and tilings (in low dimensions). Ph.D. Thesis, Technical University Munich, Germany (2003)
27. 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)