Lifts for Voronoi Cells of Lattices

Matthias Schymura[1] · Ina Seidel[2] · Stefan Weltge[2]

Abstract

Many polytopes arising in polyhedral combinatorics are linear projections of higher-dimensional polytopes with significantly fewer facets. Such lifts may yield compressed representations of polytopes, which are typically used to construct small-size linear programs. Motivated by algorithmic implications for the closest vector problem, we study lifts of Voronoi cells of lattices. We construct an explicit d-dimensional lattice such that every lift of the respective Voronoi cell has $2^{\Omega(d/\log d)}$ facets. On the positive side, we show that Voronoi cells of d-dimensional root lattices and their dual lattices have lifts with $\mathcal{O}(d)$ and $\mathcal{O}(d \log d)$ facets, respectively. We obtain similar results for spectrahedral lifts.

1 Introduction

Many polytopes that arise in the study of polyhedral combinatorics are linear projections of higher-dimensional polytopes, also called *lifts*, with significantly fewer facets. Prominent examples include basic polytopes such as permutahedra [19], cyclic polytopes [5], and polygons [44], as well as several polytopes associated to combinatorial optimization problems such as spanning tree polytopes [33, 47], subtour-elimination polytopes [48], stable set polytopes of certain families of graphs [8, 14, 39], matching polytopes of bounded-genus graphs [18], independence polytopes of regular matroids [2], or cut dominants [7].

Editor in Charge: János Pach

Matthias Schymura
schymura@b-tu.de

[1] BTU Cottbus-Senftenberg, Cottbus, Germany

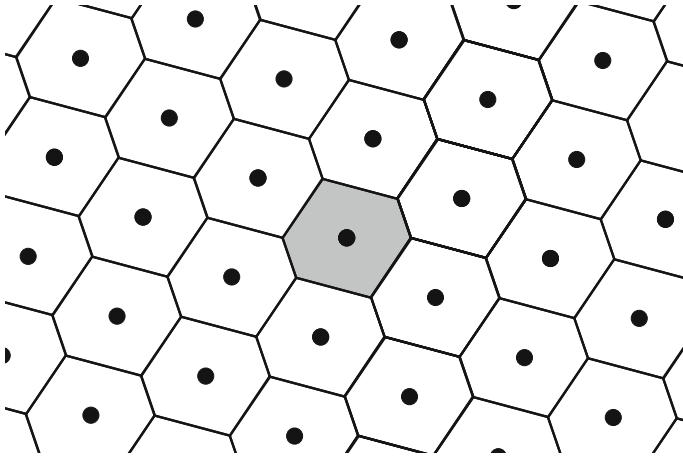[2] Technical University of Munich, Munich, Germany

Fig. 1 A lattice in $\mathbb{R}^2$ together with its Voronoi cell and the corresponding tiling of the plane via its lattice translates

In this work, we study to which extent this phenomenon also applies to Voronoi cells of lattices. Here, a *lattice* is the image of $\mathbb{Z}^k$ under an injective linear map. We say that a lattice is *k*-dimensional, if *k* is the dimension of its linear hull. The *Voronoi cell* VC(Λ) of a lattice $\Lambda \subseteq \mathbb{R}^d$ is the set of all points in lin(Λ) for which the origin is among the closest lattice points, i.e.,

$$\mathrm{VC}(\Lambda) := \{x \in \mathrm{lin}(\Lambda) : \|x\| \leq \|x - z\| \text{ for all } z \in \Lambda\},$$

where lin($\cdot$) denotes the linear hull and $\| \cdot \|$ denotes the Euclidean norm. The lattice translates $z + \mathrm{VC}(\Lambda), z \in \Lambda$, induce a facet-to-facet tiling of lin(Λ), so that in particular Voronoi cells of lattices are what is commonly called *space tiles*, see Fig. 1. Moreover, it is known that VC(Λ) is a centrally symmetric polytope with up to $2(2^d - 1)$ facets. We refer to [25, Chap. 32] for background on translative tilings of space.

It is tempting to believe that the rich structure of Voronoi cells of lattices allows to construct polytopes with significantly fewer than $2(2^d - 1)$ facets and that linearly project onto VC(Λ). In fact, this is true for several examples: A lattice whose Voronoi cell has the largest possible number of facets is the dual root lattice $A_d^\star$ (see Sect. 3.1 for a definition). However, its Voronoi cell is a permutahedron and admits a lift with only $\mathcal{O}(d \log d)$ facets [19], see Sect. 3.1. More generally, if the Voronoi cell of a *d*-dimensional lattice is a zonotope, then it has $\mathcal{O}(d^2)$ generators and hence has a lift with $\mathcal{O}(d^2)$ facets. We discuss this result in detail in Sect. 3.2.

The lattice $A_d^\star$ also belongs to the prominent class of *root lattices* and their duals. By their algebraic and geometric properties, these lattices are prime examples in various contexts: For example, they play a crucial role in Coxeter's classification of reflection groups (cf. [9, Chap. 4]), and they yield the densest sphere packings and thinnest sphere coverings in small dimensions (see [9] or [43]).

As one part of our work, we show that Voronoi cells of such lattices generally admit small lifts. In what follows, for a polytope P we write xc(P) for the minimum number

of facets of any polytope that can be linearly projected onto P. This number is called the *extension complexity* of P.

Theorem 1.1 *For every d-dimensional lattice Λ that is a root lattice or the dual of a root lattice, we have $\mathrm{xc}(\mathrm{VC}(\Lambda)) = \mathcal{O}(d \log d)$.*

This raises the question whether Voronoi cells of other lattices also have a small extension complexity, say, polynomial in their dimension. One of the main motivations for representing a polytope P as the projection of another polytope Q is that a linear optimization problem over P can be reduced to one over Q. If Q has a small number of facets, then the latter task can be expressed as a linear program with a small number of inequalities, also known as an *extended formulation*.

Thus, given a lattice $\Lambda \subseteq \mathbb{R}^d$ whose Voronoi cell has a small extension complexity, we may phrase any linear optimization problem over $\mathrm{VC}(\Lambda)$ as a small-size linear program. Such a representation may have several algorithmic consequences for the *closest vector problem*. In this problem, one is given Λ in terms of a lattice basis and a point $x \in \mathbb{R}^d$ and is asked to determine a lattice point that is closest to x, i.e., a point in

$$\mathrm{cl}(x, \Lambda) := \{z \in \Lambda : \|x - z\| \leq \|x - z'\| \text{ for all } z' \in \Lambda\}.$$

Note that $z \in \mathrm{cl}(x, \Lambda)$ if and only if $x - z \in \mathrm{VC}(\Lambda)$. Thus, a small extension complexity of $\mathrm{VC}(\Lambda)$ would yield a small-size linear program to test whether a lattice point is the closest lattice vector to x. However, in view of the fact that the closest vector problem is NP-hard [11] and the belief that NP $\neq$ coNP, we do not expect efficient algorithms that, for general lattices, decide whether a point is the closest lattice vector to x.

Another sequence of algorithmic implications arises from the algorithm of Micciancio and Voulgaris [36], which also motivated other recent work on compact representations of Voronoi cells, such as [28]. As discussed in the thesis of Hunkenschröder [27, Sect. 4.1], an optimization oracle for the Voronoi cell of a lattice is sufficient to obtain an algorithm for the closest vector problem that runs in expected polynomial time: Dadush and Bonifas [10] describe an efficient procedure to almost uniformly sample a point y from $\mathrm{VC}(\Lambda)$, which can be used to traverse the so-called Voronoi graph by a path of expected polynomial length to obtain a lattice vector that is closest to a given target point x. For sampling y, they only require a membership oracle for $\mathrm{VC}(\Lambda)$, which can be obtained from an optimization oracle [24, Sect. 6]. For traversing the Voronoi graph, it is necessary to have an efficient procedure for determining the normal of a facet of $\mathrm{VC}(\Lambda)$ that is intersected by a given line segment. Again, this can be implemented with an optimization oracle for $\mathrm{VC}(\Lambda)$. Clearly, a polynomial-size extended formulation for the Voronoi cell of a lattice yields an efficient implementation of an optimization oracle. This motivates the study of Voronoi cells of lattices for which small-size lifts can be efficiently constructed.

We remark that the mere *existence* of small size extended formulations of Voronoi cells may not be immediately applicable, since finding such representations as well as verifying that they indeed yield the Voronoi cell of a given lattice might be hard. Thus, polynomial bounds on the extension complexities of Voronoi cells of general lattices

would not contradict hardness assumptions in complexity theory. In fact, we initially considered the possibility of such bounds. However, as our main result we explicitly construct lattices with Voronoi cells of extension complexity close to the trivial upper bound $2(2^d - 1)$.

Theorem 1.2 *There exists a family of d-dimensional lattices Λ such that $\mathrm{xc}(\mathrm{VC}(\Lambda)) = 2^{\Omega(d/\log d)}$.*

Lower bounds on extension complexities have been established for various prominent polytopes in recent years. Of particular note are results for cut polytopes [6, 17, 29], matching polytopes [42], and certain stable set polytopes [21]. Lower bounds for other polytopes Q are typically obtained by showing that a face F of Q affinely projects onto one of the polytopes P from above and using the simple fact $\mathrm{xc}(P) \le \mathrm{xc}(F) \le \mathrm{xc}(Q)$. Unfortunately, it seems difficult to construct lattices for which this approach can be directly applied to the Voronoi cell. However, we will exploit the lesser known fact that $\mathrm{xc}(Q) = \mathrm{xc}(Q^\circ)$ holds for every polytope Q with the origin in its interior, where Q° is the dual polytope of Q. In fact, we will describe a way to obtain many 0/1-polytopes as projections of faces of dual polytopes of Voronoi cells of lattices. As an example, for every n-node graph G we can construct a lattice Λ of dimension at most $n + 1$ such that the stable set polytope of G is a projection of a face of $\mathrm{VC}(\Lambda)^\circ$. Theorem 1.2 then follows from a construction of Göös et al. [21] of stable set polytopes with high extension complexity.

Another prominent way of representing polytopes is via linear projections of feasible regions of *semidefinite* programs, i.e., spectrahedra. We will discuss how our approach also yields a version of Theorem 1.2 for such semidefinite lifts with a slightly weaker but still superpolynomial bound.

Outline   In Sect. 2, we provide a brief introduction to lifts of polytopes and lattices, focusing on tools and properties that are essential for our arguments in the following sections. In Sect. 3, we derive upper bounds on the extension complexity of Voronoi cells for some selected classes of lattices, such as root lattices and their duals, zonotopal lattices, and a class of lattices that do not admit a compact representation in the sense of [28]. The proof of Theorem 1.2 is given in Sect. 4, and in Sect. 5, we briefly introduce semidefinite lifts and present a version of Theorem 1.2 with a superpolynomial bound on the semidefinite extension complexity. We close our paper with a discussion of open problems in Sect. 6.

2 Preliminaries

2.1 Extension Complexity: A Toolbox

Throughout this paper we only need basic facts regarding extension complexities of polytopes and most of them are well known. For the sake of completeness, we provide proofs here. First, we start with a simple fact already mentioned in the introduction.

Lemma 2.1 *For every face F of a polytope P, we have $\mathrm{xc}(F) \le \mathrm{xc}(P)$.*

Proof If P is the image of a polyhedron Q with k facets under a linear map τ, then F is the image of $\tau^{-1}(F) \cap Q$, which is a face of Q and hence has at most k facets. $\square$

For the next fact we need the notion of a slack matrix of a polytope. To this end, we consider a polytope $P = \{x \in \mathbb{R}^d : \langle a_i, x \rangle \leq b_i, \ i \in [m]\} = \operatorname{conv}\{v_1, \ldots, v_n\}$, where $[m] := \{1, \ldots, m\}$ and $\langle \cdot, \cdot \rangle$ denotes the standard Euclidean scalar product. Corresponding to these two descriptions of P, we define the *slack matrix* $S = (S_{i,j}) \in \mathbb{R}_{\geq 0}^{m \times n}$ via $S_{i,j} = b_i - \langle a_i, v_j \rangle$. Yannakakis [48] showed that the extension complexity $\operatorname{xc}(P)$ of P equals the *nonnegative rank* of S, which is the smallest number r such that $S = FV$, where $F \in \mathbb{R}_{\geq 0}^{m \times r}$ and $V \in \mathbb{R}_{\geq 0}^{r \times n}$, and which is denoted by $r_+(S)$.

For a polytope P containing the origin $\mathbf{0}$ in its relative interior, the *dual polytope* of P is defined as

$$P^\circ := \{y \in \operatorname{lin}(P) : \langle x, y \rangle \leq 1 \text{ for all } x \in P\}.$$

It is a basic fact that P° is again a polytope with the origin in its relative interior, $\operatorname{lin}(P^\circ) = \operatorname{lin}(P)$, and $(P^\circ)^\circ = P$. Moreover, it is easy to see that if

$$P = \{x \in \operatorname{lin}(P) : \langle w_i, x \rangle \leq 1, \ i \in [m]\} = \operatorname{conv}\{v_1, \ldots, v_n\},$$

then

$$P^\circ = \{y \in \operatorname{lin}(P) : \langle v_i, x \rangle \leq 1, \ i \in [n]\} = \operatorname{conv}\{w_1, \ldots, w_m\}. \tag{1}$$

In particular, this shows that if S is a slack matrix of P induced by $v_1, \ldots, v_n$ and $w_1, \ldots, w_m$, then S^{T} is a slack matrix of P°. Since $r_+(S) = r_+(S^{\mathsf{T}})$ we obtain the following fact.

Lemma 2.2 *For every polytope $P \subseteq \mathbb{R}^d$ that contains the origin in its relative interior, we have*

$$\operatorname{xc}(P) = \operatorname{xc}(P^\circ).$$

The next statement shows that the extension complexity behaves well under Cartesian products, Minkowski sums, and intersections.

Lemma 2.3 *If $P \subseteq \mathbb{R}^d$, $Q \subseteq \mathbb{R}^{d'}$ are polytopes, then*

(i) $\operatorname{xc}(P \times Q) \leq \operatorname{xc}(P) + \operatorname{xc}(Q)$.

Moreover, if $d = d'$, then

(ii) $\operatorname{xc}(P + Q) \leq \operatorname{xc}(P) + \operatorname{xc}(Q)$ *and*
(iii) $\operatorname{xc}(P \cap Q) \leq \operatorname{xc}(P) + \operatorname{xc}(Q)$.

Proof (i): If P' linearly projects onto P and Q' onto Q, then $P' \times Q'$ linearly projects onto $P \times Q$. Moreover, the number of facets of $P' \times Q'$ is equal to the sum of the number of facets of P' and Q'.

(ii): The polytope $P \times Q$ linearly projects onto $P + Q$ via $(p, q) \mapsto p + q$ for $(p, q) \in P \times Q$, and hence the claim follows from (i).

(iii): If $P = \pi(P')$ and $Q = \tau(Q')$ hold for some polyhedra P', Q' and linear maps π, τ, then $P \cap Q$ is a linear image of the polyhedron $L = \{(y, z) \in P' \times Q' : \pi(y) = \tau(z)\}$. Moreover, the number of facets of L is at most the number of facets of $P' \times Q'$, which, again, is equal to the sum of the number of facets of P' and Q'.   □

The next fact is a very useful result following from a work of Balas [3] deriving a description of the convex hull of the union of certain polytopes. The proof of the version presented here can be found in [46, Prop. 3.1.1].

Lemma 2.4 *Let $P_1, \ldots, P_k$ be polytopes, then*

$$\mathrm{xc}\left(\mathrm{conv}\left(P_1 \cup \ldots \cup P_k\right)\right) \leq \sum_{i=1}^{k} \mathrm{xc}(P_i) + |\{i \in [k] : \dim(P_i) = 0\}|.$$

We mentioned already that some lattices have a permutahedron as their Voronoi cell. These polytopes arise from a single vector by permuting its coordinates in all possible ways and taking their convex hull. Let us denote the set of all bijective maps on $[d]$ by S_d. For a permutation $\pi \in S_d$ and a vector $v = (v(1), \ldots, v(d)) \in \mathbb{R}^d$, let $\pi(v) := (v(\pi(1)), \ldots, v(\pi(d)))$ be the vector that arises from v via permuting its entries according to π.

Lemma 2.5 *For every $v \in \mathbb{R}^d$ we have* $\mathrm{xc}\left(\mathrm{conv}\{\pi(v) : \pi \in S_d\}\right) \leq d^2$.

Proof For $\pi \in S_d$, let $P(\pi) \in \{0, 1\}^{d \times d}$ with $P(\pi)_{ij} = 1$ if and only if $\pi(i) = j$, for all $i, j \in [d]$, be the associated permutation matrix. It is easy to see that $\mathrm{conv}\{\pi(v) : \pi \in S_d\}$ is the image of $B_d := \mathrm{conv}\{P(\pi) : \pi \in S_d\}$ under the linear map $\tau : \mathbb{R}^{d \times d} \to \mathbb{R}^d$ with $\tau(X)_i = \sum_{j=1}^{d} v_j X_{ij}$, for $i \in [d]$. The latter polytope is the *Birkhoff–von Neumann polytope* [4, 38] described via

$$B_d = \left\{ X \in \mathbb{R}_{\geq 0}^{d \times d} : \sum_{i=1}^{d} X_{ij} = 1 \text{ for } j \in [d], \sum_{j=1}^{d} X_{ij} = 1 \text{ for } i \in [d] \right\},$$

which has d^2 facets.   □

Goemans [19] showed that if $v = (1, 2, \ldots, d)$, then the above bound can be improved to $\mathrm{xc}\left(\mathrm{conv}\{\pi(v) : \pi \in S_d\}\right) = \Theta(d \log d)$.

2.2 Lattices and Voronoi Cells

Most basic notions regarding lattices and their Voronoi cells have been already introduced in Sect. 1. In this section, we provide some further definitions and results that we use to obtain bounds on the extension complexity of Voronoi cells of lattices.

We call two lattices $\Lambda, \Gamma \subseteq \mathbb{R}^d$ *isomorphic*, if there exists an orthogonal matrix $Q \in \mathbb{R}^{d \times d}$ such that $Q\Lambda = \Gamma$. Note that $\mathrm{VC}(\Gamma) = Q\,\mathrm{VC}(\Lambda)$ and therefore the extension complexities of their Voronoi cells coincide. In some parts, we will consider the *dual lattice* of a lattice $\Lambda \subseteq \mathbb{R}^d$, which is defined as

$$\Lambda^{\star} = \{x \in \mathrm{lin}(\Lambda) : \langle x, y \rangle \in \mathbb{Z} \text{ for all } y \in \Lambda\}.$$

Note that for every two lattices Λ, Γ, their product $\Lambda \times \Gamma$ is also a lattice. The following lemma shows that the Cartesian product behaves well with respect to Voronoi cells or duals of lattices.

Lemma 2.6 *For any two lattices $\Lambda \subseteq \mathbb{R}^d$ and $\Gamma \subseteq \mathbb{R}^{d'}$ we have*

(i) $\mathrm{VC}(\Lambda \times \Gamma) = \mathrm{VC}(\Lambda) \times \mathrm{VC}(\Gamma)$ *and*
(ii) $(\Lambda \times \Gamma)^{\star} = \Lambda^{\star} \times \Gamma^{\star}$.

Proof The first claim follows since

$$\begin{aligned}
\mathrm{VC}(\Lambda \times \Gamma) = \{(x, y) &\in \mathrm{lin}(\Lambda \times \Gamma) : \\
&\|(x, y)\|^2 \leq \|(x, y) - (w, z)\|^2 \text{ for all } (w, z) \in \Lambda \times \Gamma\} \\
= \{(x, y) &: x \in \mathrm{lin}(\Lambda), \ y \in \mathrm{lin}(\Gamma), \\
&\|x\|^2 + \|y\|^2 \leq \|x - w\|^2 + \|y - z\|^2 \text{ for all } (w, z) \in \Lambda \times \Gamma\} \\
= \{(x, y) &: x \in \mathrm{lin}(\Lambda), \ y \in \mathrm{lin}(\Gamma), \\
&\|x\|^2 \leq \|x - w\|^2 \text{ for all } w \in \Lambda, \ \|y\|^2 \leq \|y - z\|^2 \text{ for all } z \in \Gamma\} \\
= \mathrm{VC}(\Lambda) &\times \mathrm{VC}(\Gamma)
\end{aligned}$$

holds. For the second claim, it is clear that $\Lambda^{\star} \times \Gamma^{\star} \subseteq (\Lambda \times \Gamma)^{\star}$ holds. To see that the reverse inclusion holds as well, let $(x, y) \in (\Lambda \times \Gamma)^{\star}$. For every $w \in \Lambda$, we have $(w, \mathbf{0}) \in \Lambda \times \Gamma$ and hence $\langle x, w \rangle = \langle (x, y), (w, \mathbf{0}) \rangle \in \mathbb{Z}$. This yields $x \in \Lambda^{\star}$. We obtain $y \in \Gamma^{\star}$ in an analogous fashion. $\square$

A main ingredient for proving Theorem 1.2 is to consider the dual polytope $\mathrm{VC}(\Lambda)^{\circ}$ of $\mathrm{VC}(\Lambda)$. Recall that we have $\mathrm{xc}(\mathrm{VC}(\Lambda)) = \mathrm{xc}(\mathrm{VC}(\Lambda)^{\circ})$ by Lemma 2.2. The following two observations are crucial for our arguments.

Lemma 2.7 *For every lattice Λ we have*

$$\mathrm{VC}(\Lambda)^{\circ} = \mathrm{conv}\left\{\frac{2}{\|z\|^2} z : z \in \Lambda \setminus \{\mathbf{0}\}\right\}.$$

Proof In view of the identities

$$\begin{aligned}
\mathrm{VC}(\Lambda) &= \{x \in \mathrm{lin}(\Lambda) : \|x\|^2 \leq \|x - z\|^2 \text{ for all } z \in \Lambda\} \\
&= \left\{x \in \mathrm{lin}(\Lambda) : \langle x, z \rangle \leq \frac{\|z\|^2}{2} \text{ for all } z \in \Lambda\right\}
\end{aligned}$$

$$= \left\{ x \in \mathrm{lin}(\Lambda) : \left\langle x, \frac{2}{\|z\|^2} z \right\rangle \le 1 \text{ for all } z \in \Lambda \setminus \{\mathbf{0}\} \right\},$$

the claim follows from (1).   □

Lemma 2.8 *Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice and $p \in \mathbb{R}^d$. If $\mathbf{0} \in \mathrm{cl}(p, \Lambda)$, then*

$$\mathrm{conv}\left\{ \frac{2}{\|z\|^2} z : z \in \mathrm{cl}(p, \Lambda) \setminus \{\mathbf{0}\} \right\}$$

is a face of $\mathrm{VC}(\Lambda)^\circ$.

Proof Since $\mathbf{0} \in \mathrm{cl}(p, \Lambda)$, every nonzero lattice point $z \in \Lambda \setminus \{\mathbf{0}\}$ satisfies $\|p - z\|^2 \ge \|p\|^2$, with equality if and only if $z \in \mathrm{cl}(p, \Lambda) \setminus \{\mathbf{0}\}$. Note that the above inequality is equivalent to $\langle p, (2/\|z\|^2)z \rangle \le 1$. Thus, due to Lemma 2.7 we see that $F := \{y \in \mathrm{VC}(\Lambda)^\circ : \langle p, y \rangle = 1\}$ is a face of $\mathrm{VC}(\Lambda)^\circ$. This establishes the claim since

$$F = \mathrm{conv}\left\{ \frac{2}{\|z\|^2} z : z \in \Lambda \setminus \{\mathbf{0}\}, \left\langle p, \frac{2}{\|z\|^2} z \right\rangle = 1 \right\}$$

$$= \mathrm{conv}\left\{ \frac{2}{\|z\|^2} z : z \in \mathrm{cl}(p, \Lambda) \setminus \{\mathbf{0}\} \right\}. \qquad \square$$

3 Lattices with Small Extension Complexity

In this section, we provide bounds on the extension complexities of Voronoi cells of some prominent lattices.

3.1 Root Lattices and Their Duals

We start with Voronoi cells of root lattices and their duals. An *irreducible root lattice* is a lattice Λ for which there exists a finite set S of vectors of squared length equal to 1 or 2, such that $\Lambda = \left\{ \sum_{b \in S} \alpha_b b : \alpha_b \in \mathbb{Z} \text{ for all } b \in S \right\}$. We say that a lattice is a (*general*) *root lattice*, if it is isomorphic to a lattice obtained by iteratively taking Cartesian products with irreducible root lattices. A well-known theorem related to the classification of reflection groups states that besides the lattice $\mathbb{Z}^d$ of integers, up to isomorphism the irreducible root lattices split into the two infinite classes

$$A_d = \{x \in \mathbb{Z}^{d+1} : x(1) + \cdots + x(d+1) = 0\} \quad \text{and}$$
$$D_d = \{x \in \mathbb{Z}^d : x(1) + \cdots + x(d) \text{ is even}\},$$

and the three exceptional lattices

$$E_8 = D_8 \cup \left(\frac{1}{2}\mathbf{1} + D_8 \right),$$
$$E_7 = \{x \in E_8 : \langle x, e_7 + e_8 \rangle = 0\}, \quad \text{and}$$

$$E_6 = \{x \in E_7 : \langle x, e_6 + e_8 \rangle = 0\}.$$

Here and in the following, we denote by e_i the ith standard Euclidean unit vector and by $\mathbf{1}$ the all-one vector in the corresponding space. Moreover, the dual lattices of the two infinite classes A_d and D_d are given by

$$A_d^\star = \bigcup_{i=0}^{d} (v_i + A_d),$$

with

$$v_i = \Big(\underbrace{\frac{i}{d+1}, \dots, \frac{i}{d+1}}_{j \text{ times}}, \underbrace{-\frac{j}{d+1}, \dots, -\frac{j}{d+1}}_{i \text{ times}}\Big),$$

for $0 \leq i \leq d$ and $j = d + 1 - i$, and

$$D_d^\star = \mathbb{Z}^d \cup \left(\frac{1}{2}\mathbf{1} + \mathbb{Z}^d\right),$$

respectively. In the literature the dual $D_d^\star$ is usually scaled by a factor of 2 in order to get an integral lattice, which is often more convenient to investigate. In order to avoid confusion, we denote it by

$$\bar{D}_d^\star := 2D_d^\star = (2\mathbb{Z}^d) \cup (\mathbf{1} + 2\mathbb{Z}^d),$$

and note that this scaling has no effect on the extension complexity of its Voronoi cell. We refer to Conway and Sloane [9, Chaps. 4 and 21] and Martinet [34, Chap. 4] for proofs, original references and background information on root lattices. Details on Voronoi cells and Delaunay polytopes of root lattices can be found in Moody and Patera [37], which together with the two aforementioned monographs are our main sources of information.

Given a lattice $\Lambda \subseteq \mathbb{R}^d$ we write $|\Lambda| = \min\{\|z\| : z \in \Lambda \setminus \{\mathbf{0}\}\}$ for the length of a shortest non-trivial vector in Λ. A *minimal vector* of Λ is any vector $z \in \Lambda$ with $\|z\| = |\Lambda|$, and a *facet vector* of Λ is any vector $w \in \Lambda$, such that the constraint $\langle x, w \rangle \leq \|w\|^2/2$ defines a facet of the Voronoi cell $\mathrm{VC}(\Lambda)$. For convenience, we write

$$\mathcal{S}(\Lambda) = \{z \in \Lambda : \|z\| = |\Lambda|\} \quad \text{and} \quad \mathcal{F}(\Lambda) = \{w \in \Lambda : w \text{ is a facet vector of } \Lambda\},$$

for the set of minimal vectors and facet vectors, respectively. In general, one has the inclusion $\mathcal{S}(\Lambda) \subseteq \mathcal{F}(\Lambda)$, which however is usually strict. Root lattices are now neatly characterized by the property that every facet vector is at the same time a minimal vector, that is, the equality $\mathcal{S}(\Lambda) = \mathcal{F}(\Lambda)$ holds (see Rajan and Shende [40]).

Since the set of minimal vectors of the irreducible root lattices are well understood, this allows to describe their Voronoi cells as well. For the sake of the asymptotic study of the extension complexity of their Voronoi cells, it suffices to understand the two infinite families A_d and D_d, and their duals $A_d^\star$ and $D_d^\star$. In the sequel, we provide bounds on the extension complexities of the Voronoi cells of these lattices. To achieve these bounds, we sometimes use a characterization of the facet vectors and in other cases we use a characterization of the vertices of the Voronoi cell. For the sake of easy reference, we describe the vertices and facet vectors in all cases. Due to Lemmas 2.3 and 2.6, these bounds directly imply Theorem 1.1. Moreover, the bound in Theorem 1.1 is asymptotically tight since the Voronoi cell of $A_d^\star$ is a permutahedron, see Lemma 3.3.

3.1.1 Voronoi Cell of A_d

The Voronoi cell of the root lattice A_d is given by

$$VC(A_d) = \text{conv}\{\pi(v_i) : \pi \in S_{d+1}, \, i \in \{0, \ldots, d\}\},$$

where

$$v_i = \Big(\underbrace{\frac{i}{d+1}, \ldots, \frac{i}{d+1}}_{j \text{ times}}, \underbrace{-\frac{j}{d+1}, \ldots, -\frac{j}{d+1}}_{i \text{ times}}\Big) \in \mathbb{R}^{d+1}$$

with $j = d+1-i$. Moreover, we have

$$VC(A_d) = \{x \in \mathbb{R}^{d+1} : \langle x, z \rangle \le 1 \text{ for all } z \in \mathcal{F}(A_d)\}, \quad \text{where}$$
$$\mathcal{F}(A_d) = \{\pi((1, -1, 0, \ldots, 0)) : \pi \in S_{d+1}\}$$

(see [9, Chaps. 21 and 4, Sect. 6]).

Lemma 3.1 $xc(VC(A_d)) = \mathcal{O}(d)$.

Proof Using the description of the facet vectors stated above, we obtain that $VC(A_d)^\circ = S + (-S)$, where S is the d-dimensional simplex $S = \text{conv}\{e_1, \ldots, e_{d+1}\}$. Hence, using Lemmas 2.3 and 2.7, we obtain the upper bound $xc(VC(A_d)) \le 2(d+1)$. $\square$

3.1.2 Voronoi Cell of D_d

The Voronoi cell of D_d is given by

$$VC(D_d) = \text{conv}\left(\{\pm e_1, \ldots, \pm e_d\} \cup \left\{-\frac{1}{2}, \frac{1}{2}\right\}^d\right).$$

Moreover, we have

$$\mathrm{VC}(D_d) = \{x \in \mathbb{R}^{d+1} : \langle x, z \rangle \leq 1 \text{ for all } z \in \mathcal{F}(D_d)\}, \quad \text{where}$$
$$\mathcal{F}(D_d) = \{\pm e_i \pm e_j : 1 \leq i < j \leq d\}.$$

This follows from the characterization of the minimal (and thus facet) vectors of D_d given in [9, Chap. 4, Sect. 7]. The inner description of the Voronoi cell can be read off from the vertices of a fundamental simplex for D_d (see [9, Chap. 21, Fig. 21.7]).

Lemma 3.2 $\mathrm{xc}(\mathrm{VC}(D_d)) = \mathcal{O}(d).$

Proof Using the description of the vertices of $\mathrm{VC}(D_d)$ stated above, we obtain that

$$\mathrm{VC}(D_d)^\circ = 2 \cdot \mathrm{conv} \{\pm e_1, \ldots, \pm e_d\} \cap [-1, 1]^d.$$

Hence, the dual of the Voronoi cell is the intersection of a hypercube and a crosspolytope. Since

$$\mathrm{xc}([-1, 1]^d) = \mathrm{xc}(\mathrm{conv}\{\pm e_1, \ldots, \pm e_d\}) = 2d, \tag{2}$$

(see, e.g., [23, Cor. 2.5]), Lemmas 2.3 and 2.7 imply $\mathrm{xc}(\mathrm{VC}(D_d)) = \mathcal{O}(d)$. □

3.1.3 Voronoi Cell of $A_d^\star$

The Voronoi cell of the dual of the root lattice $A_d^\star$ is given by

$$\mathrm{VC}(A_d^\star) = \mathrm{conv}\{\pi(v) : \pi \in S_{d+1}\},$$

where

$$v = \frac{1}{2d+2}(-d, -d+2, \ldots, d-2, d) \in \mathbb{R}^{d+1}.$$

Moreover, we have

$$\mathcal{F}(A_d^\star) = \{v \in \mathrm{lin}(A_d^\star) : v \text{ is a vertex of } \mathrm{VC}(A_d)\}.$$

The characterization of the vertices can be found in [9, Chap. 21, Sect. 3F] and the fact that the facet vectors are exactly the vertices of $\mathrm{VC}(A_d)$ is explained in detail in the unpublished monograph [12, Chap. 3.5].

Lemma 3.3 $\mathrm{xc}(\mathrm{VC}(A_d^\star)) = \Theta(d \log d).$

Proof Using the description of the vertices of $\mathrm{VC}(A_d^\star)$ stated before, we obtain that $\mathrm{VC}(A_d^\star)$ is an affine linear transformation of the standard permutahedron

$$P_d = \{(\pi(1), \ldots, \pi(d+1)) : \pi \in S_{d+1}\}.$$

In fact,

$$\mathrm{VC}(A_d^\star) = \frac{1}{d+1} P_d - \frac{d+2}{2d+2} \mathbf{1}.$$

The claim follows, since Goemans [19] showed that the extension complexity of P_d is in $\Theta(d \log d)$. $\square$

3.1.4 Voronoi Cell of $D_d^\star$

As explained before, we consider the integral lattice $\bar{D}_d^\star$ instead of $D_d^\star$. The Voronoi cell of $\bar{D}_d^\star$ is given by

$$\mathrm{VC}(\bar{D}_d^\star) = \mathrm{conv}\,\{\pi(v) : \pi \in S_d, v \in V\},$$

where

$$V = \begin{cases} \{0\}^{d/2} \times \{-1, 1\}^{d/2} & \text{if } d \text{ is even,} \\ \{0\}^{(d-1)/2} \times \left\{-\dfrac{1}{2}, \dfrac{1}{2}\right\} \times \{-1, 1\}^{(d-1)/2} & \text{if } d \text{ is odd.} \end{cases}$$

Moreover, we have

$$\mathcal{F}(\bar{D}_d^\star) = \{\pm 2e_1, \dots, \pm 2e_d\} \cup \{-1, 1\}^d.$$

We refer to [9, Chap. 21, Sect. 3E] for the characterization of the facet vectors and the inner description of the Voronoi cell, which is therein denoted by the symbols $\beta(d, d/2)$, for d even, and $\delta(d, (d-1)/2)/2$, for d odd.

Lemma 3.4 $\mathrm{xc}(\mathrm{VC}(D_d^\star)) = \mathcal{O}(d)$.

Proof Using the above description of the facet vectors, we obtain that

$$\mathrm{VC}(\bar{D}_d^\star) = [-1, 1]^d \cap \left(\frac{d}{2} \cdot \mathrm{conv}\,\{\pm e_1, \dots, \pm e_d\}\right).$$

Hence, the Voronoi cell of $D_d^\star$ is the intersection of a hypercube and a crosspolytope. As in the case of the root lattice D_d, the stated bound follows by Lemma 2.3 and (2). $\square$

Note that all the bounds stated in Lemmas 3.1, 3.2, and 3.4 are asymptotically tight, since the extension complexity of a polytope grows at least linearly with its dimension (cf. [15, Eq. 2 and Prop. 5.2]).

3.2 Zonotopal Lattices

A *zonotope* $Z \subseteq \mathbb{R}^d$ is the Minkowski sum of finitely many line segments, that is, there are vectors $a_1, b_1, \ldots, a_m, b_m \in \mathbb{R}^d$ such that $Z = \sum_{i=1}^{m} \text{conv} \{a_i, b_i\}$. The non-zero vectors $z_i = b_i - a_i$ are usually called the *generators* of the zonotope, and clearly, Z is an affine projection of the m-dimensional cube $[-1, 1]^m$ via $e_i \mapsto z_i$, for $1 \leq i \leq m$, and a suitable translation. Regarding the extension complexity of a zonotope Z, the bound $\text{xc}(Z) \leq 2m$ thus immediately follows from the definition.

A lattice $\Lambda \subseteq \mathbb{R}^d$ is said to be *zonotopal* if its Voronoi cell is a zonotope. Every lattice of dimension at most three is zonotopal, but from dimension four on there exist non-zonotopal lattices. For instance, the Voronoi cell of the root lattice D_4 is the non-zonotopal 24-cell. Examples of classes of zonotopal lattices are $\mathbb{Z}^d$, the root lattice A_d, its dual lattice $A_d^\star$, lattices of Voronoi's first kind, and the tensor product $A_d \otimes A_{d'}$. Zonotopal space tiles have been extensively studied over the years, mostly due to their combinatorial connections to regular matroids, hyperplane arrangements, and totally unimodular matrices. For a detailed account on zonotopal lattices and pointers to the original works containing the previous statements we refer to [35, Sect. 2].

The tiling constraint on a zonotope that arises as the Voronoi cell of a lattice, allows it to have at most quadratically many generators in terms of its dimension. In particular, these polytopes admit lifts with quadratically many facets.

Theorem 3.5 *Each zonotopal lattice $\Lambda \subseteq \mathbb{R}^d$ satisfies* $\text{xc}(\text{VC}(\Lambda)) \leq d(d + 1)$.

Proof It suffices to argue that the Voronoi cell is generated by at most $\binom{d+1}{2}$ line segments. Indeed, each line segment L satisfies $\text{xc}(L) = 2$ and hence the statement follows using Lemma 2.3.

Erdahl [13, Sect. 5] proved that the generators of a space tiling zonotope correspond to the normal vectors of a certain dicing. A *dicing* in $\mathbb{R}^d$ is an arrangement of hyperplanes consisting of $r \geq d$ families of infinitely many equally spaced hyperplanes such that: (a) there are d families whose corresponding normal vectors are linearly independent, and (b) every vertex of the arrangement is contained in a hyperplane of each family.

By [13, Thm. 3.3], every dicing is affinely equivalent to a dicing whose set of hyperplane normal vectors-one normal vector for each of the r families-consists of the columns of a totally unimodular $d \times r$ matrix. By construction, this totally unimodular matrix is such that for any two of its columns v, w, we have $v \neq \pm w$ and $v, w \neq \mathbf{0}$. A classical result, that is often attributed to Heller [26] but already appears in Korkine and Zolotarev [31], yields that every such totally unimodular $d \times r$ matrix has at most $r \leq \binom{d+1}{2}$ columns. Thus, the zonotopal Voronoi cell $\text{VC}(\Lambda)$ is generated by at most $\binom{d+1}{2}$ line segments.   □

Alternatively, the fact that zonotopal Voronoi cells in $\mathbb{R}^d$ are generated by at most $\binom{d+1}{2}$ line segments also follows from Voronoi's reduction theory. The Delaunay subdivisions of zonotopal lattices correspond to certain polyhedral cones (Voronoi's L-types) in the cone $\mathcal{S}_{\geq 0}^d$ of positive semi-definite $d \times d$ matrices that are generated by rank one matrices. Since $\mathcal{S}_{\geq 0}^d$ has dimension $\binom{d+1}{2}$, Carathéodory's Theorem yields

the bound. We refer the reader to Erdahl [13, Sect. 7] for an intuitive description and references to the original works.

3.3 Lattices Defined by Simple Congruences

For any $a \in \mathbb{N}$, we consider the lattice

$$\Lambda_d(a) := \{x \in \mathbb{Z}^d : x_1 \equiv x_2 \equiv \ldots \equiv x_d \bmod a\}. \tag{3}$$

The case $a = \lceil d/2 \rceil$ played a special role in [28, Thm. 2] for the determination of lattices that do not have a basis that admits a compact representation of the Voronoi cell. To this end, the authors determined the set $\mathcal{F}(\Lambda_d(\lceil d/2 \rceil))$ of facet vectors explicitly (there are exponentially many of them). However, their proof can be extended to general a to give a description of the facet vectors of $\mathcal{F}(\Lambda_d(a))$ that is precise enough to allow drawing conclusions towards small extended formulations.

Lemma 3.6 *For all $a \in \mathbb{N}$, the set of facet vectors of $\Lambda_d(a)$ is contained in*

$$\mathcal{F}(\Lambda_d(a)) \subseteq \{\mathbf{1}, -\mathbf{1}\} \cup \{\pm a e_i : i \in [d]\}$$
$$\cup \left\{ v_{S,\ell} \in \mathbb{R}^d : \emptyset \neq S \subsetneq [d], \ \ell \in \left\{ \left\lfloor \frac{a|S|}{d} \right\rfloor, \left\lceil \frac{a|S|}{d} \right\rceil \right\} \right\},$$

where $v_{S,\ell}(i) = a - \ell$, if $i \in S$, and $v_{S,\ell}(i) = -\ell$, if $i \notin S$.

Proof Follows directly with the proof of [28, Lem. 3]. □

Theorem 3.7 *For all $a \in \mathbb{N}$, we have $\mathrm{xc}(\mathrm{VC}(\Lambda_d(a))) \in \mathcal{O}(d^3)$.*

Proof Due to Lemma 3.6 and (1), the dual polytope of the Voronoi cell of $\Lambda_d(a)$ equals

$$\mathrm{VC}(\Lambda_d(a))^\circ = \mathrm{conv}\left(V_{\pm \mathbf{1}} \cup V_{\pm a} \cup \bigcup_{k,\ell} V_{k,\ell} \right),$$

where the last union is over all $k \in [d-1]$, $\ell \in \{\lfloor ak/d \rfloor, \lceil ak/d \rceil\}$, and the sets $V_{\pm \mathbf{1}}$, $V_{\pm a}$, and $V_{k,\ell}$ are defined as follows:

$$V_{\pm \mathbf{1}} := \mathrm{conv}\left\{ \frac{2}{d}\mathbf{1}, -\frac{2}{d}\mathbf{1} \right\}, \quad V_{\pm a} := \mathrm{conv}\left\{ \pm\frac{2}{a^2} a e_i : i \in [d] \right\}, \quad \text{and}$$

$$V_{k,\ell} := \mathrm{conv}\Bigg\{ \frac{2}{k\,(a-\ell)^2 + (d-k)\,\ell^2} z : z \in \{a-\ell, -\ell\}^d$$
$$\text{with exactly } k \text{ entries equal to } a - \ell \Bigg\}.$$

Clearly, $\mathrm{xc}(V_{\pm \mathbf{1}}) = 2$. Moreover, $\mathrm{xc}(V_{\pm a}) = 2d$, since $V_{\pm a}$ is a crosspolytope, see (2). Furthermore, for $k \in [d-1]$ and $\ell \in \{\lfloor ak/d \rfloor, \lceil ak/d \rceil\}$, using Lemma 2.5 and the fact that $V_{k,\ell}$ equals

$$V_{k,\ell} = \mathrm{conv}\,\{\pi(v_{k,\ell}) : \pi \in S_d\},$$

where $v_{k,\ell}(a-\ell, \ldots, a-\ell, -\ell, \ldots, -\ell)$ with exactly k entries equal to $a-\ell$, we obtain $\mathrm{xc}(V_{k,\ell}) \le d^2$. Combining these bounds and applying Lemmas 2.4 and 2.2, we obtain the desired bound.   □

4 Lower Bounds on the Extension Complexity of Voronoi Cells

The aim of this section is to prove Theorem 1.2. Inspired by Kannan's proof [30, Sect. 6] of the NP-hardness of the closest vector problem, for every 0/1-polytope P we are able to construct a lattice such that a face of its dual Voronoi cell projects onto P. To obtain a lattice of small dimension, P needs to fulfill some extra condition.

Lemma 4.1 *Let $H \subseteq \mathbb{R}^k$ be an affine subspace such that all vectors in $X := \{0,1\}^k \cap H$ have the same norm. There is a lattice Λ with $\dim(\Lambda) \le \dim(H)+1$ such that $\mathrm{conv}(X)$ is a linear projection of a face of $\mathrm{VC}(\Lambda)^\circ$.*

Proof Let $\alpha \ge 0$ be such that $\|x\| = \alpha$ for all $x \in X$. We may assume that H is nonempty and that $\alpha > 0$, otherwise $\mathrm{conv}(X)$ is empty or consists of a single point, in which case the claim is trivial. Let $h \in H$ and let L be the linear subspace such that $H = L + h$. Consider the lattice

$$\Lambda := \left\{ z = (z', z'') \in \mathbb{Z}^k \times \alpha\mathbb{Z} : z' + \frac{1}{\alpha} z'' h \in L, \ \langle \mathbf{1}, z' \rangle + \alpha z'' = 0 \right\}$$

and let $p := (\mathbf{0}, -\alpha) \in \mathbb{R}^{k+1}$. We will show that

$$\mathrm{cl}(p, \Lambda) = \{\mathbf{0}\} \cup \{(x, -\alpha) : x \in X\} =: U \tag{4}$$

holds. By Lemma 2.8, this will imply that

$$\mathrm{conv}\left\{ \frac{2}{\|(x, -\alpha)\|^2} (x, -\alpha) : x \in X \right\} = \mathrm{conv}\left\{ \frac{1}{\alpha^2} (x, -\alpha) : x \in X \right\}$$

is a face of $\mathrm{VC}(\Lambda)^\circ$ that linearly projects onto $\mathrm{conv}(X)$.

First note that $U \subseteq \Lambda$. Moreover, we have $\|p - \mathbf{0}\| = \alpha$ and for each $x \in X$ we have $\|p - (x, -\alpha)\| = \|x\| = \alpha$. Thus, in order to establish (4) it remains to show that every lattice point $z = (z', z'') \in \Lambda \setminus U$ satisfies $\alpha < \|p - z\|$. Equivalently, we have to show that every such point satisfies

$$f(z) := \|z'\|^2 + \|z'' + \alpha\|^2 > \alpha^2. \tag{5}$$

This is clear if $z'' \notin \{0, -\alpha, -2\alpha\}$. If $z'' = 0$, then since $z \notin U$ we must have $z' \neq \mathbf{0}$ and hence $f(z) = \|z'\|^2 + \alpha^2 > \alpha^2$. If $z'' = -\alpha$, then $z' \in H$ and $\langle \mathbf{1}, z' \rangle = \alpha^2$ hold. Since $z' \in \mathbb{Z}^k$, we obtain $f(z) = \|z'\|^2 \geq \langle \mathbf{1}, z' \rangle = \alpha^2$ with equality only if $z' \in \{0, 1\}^k$. However, in the latter case we would have $z' \in \{0, 1\}^k \cap H = X$ and hence $z \in U$, a contradiction. Thus, we obtain (5). Finally, if $z'' = -2\alpha$, then $f(z) = \|z'\|^2 + \alpha^2$ and $\langle \mathbf{1}, z' \rangle = 2\alpha^2 > 0$, implying $z' \neq \mathbf{0}$ and hence (5) holds.   □

While the previous lemma appears quite restrictive, the next lemma shows that we may apply it to a large class of 0/1-polytopes.

Lemma 4.2 *Let $X = \{x \in \{0, 1\}^k : Ax \leq b\}$, for some $A \in \mathbb{R}^{m \times k}$, $b \in \mathbb{R}^m$ such that $b - Ax \in \{0, 1\}^m$, for all $x \in X$. There is a lattice Λ of dimension at most $k + 1$ such that $\mathrm{conv}(X)$ is the linear projection of a face of $\mathrm{VC}(\Lambda)^\circ$.*

Proof Consider the set

$$X' := \{(x, x', s, s') \in \{0, 1\}^{k+k+m+m} : Ax + s = b, \ x + x' = \mathbf{1}, \ s + s' = \mathbf{1}\}$$

and observe that projecting X' onto the first k coordinates yields the set X. Moreover, notice that every vector in X' consists of exactly $k + m$ ones. In other words, the norm of every vector in X' is $\sqrt{k + m}$ and hence, we may apply Lemma 4.1 to obtain a lattice Λ with dimension at most $k + 1$ such that $\mathrm{conv}(X')$ is the linear projection of a face F of $\mathrm{VC}(\Lambda)^\circ$. Since $\mathrm{conv}(X)$ is a linear projection of $\mathrm{conv}(X')$, we see that $\mathrm{conv}(X)$ is also a linear projection of F.   □

Proof of Theorem 1.2 We use a result of Göös et al. [21] that yields a family of n-node graphs G such that the stable set polytope P_G of G satisfies $\mathrm{xc}(P_G) = 2^{\Omega(n/\log n)}$. Let $X \subseteq \{0, 1\}^n$ denote the set of characteristic vectors of stable sets in G. Notice that

$$X = \{x \in \{0, 1\}^n : x(i) + x(j) \leq 1 \text{ for all } \{i, j\} \in E(G)\}.$$

By Lemma 4.2, there is a d-dimensional lattice Λ with $d \leq n + 1$ such that $\mathrm{conv}(X)$ is a linear projection of a face F of $\mathrm{VC}(\Lambda)^\circ$. We conclude

$$\mathrm{xc}(\mathrm{VC}(\Lambda)) = \mathrm{xc}(\mathrm{VC}(\Lambda)^\circ) \geq \mathrm{xc}(F) \geq \mathrm{xc}(\mathrm{conv}(X)) = \mathrm{xc}(P_G) = 2^{\Omega(n/\log n)},$$

and the claim follows since $d = \mathcal{O}(n)$.   □

5 Spectrahedral Lifts

A generalization of linear lifts of a polytope is the following. By $\mathcal{S}^m$ we denote the set of all symmetric, real $m \times m$ matrices. Moreover, by $\mathcal{S}_+^m$ we denote the set of all those matrices in $\mathcal{S}^m$ that are positive semidefinite (PSD). A *spectrahedron* is a set containing all vectors $x \in \mathbb{R}^n$ that fulfill conditions of the form $M(x) \in \mathcal{S}_+^m$, where $M : \mathbb{R}^n \to \mathcal{S}^m$ is an affine function. For a polytope P, the pair (Q, π), where $Q \subseteq \mathbb{R}^n$ is a spectrahedron and $\pi : \mathbb{R}^n \to \mathbb{R}^d$ is an affine map with $\pi(Q) = P$, is called a

(*PSD*) *lift* of P. The *size* of this lift refers to the dimension of the matrix $M(x)$. For $Q = \{x \in \mathbb{R}^n : M(x) \in \mathcal{S}^m_+\}$ the size equals m. The *semidefinite extension complexity* of P, denoted by $\mathrm{sxc}(P)$, is defined as the smallest size of any of its (PSD) lifts.

Given a polyhedron $Q = \{x \in \mathbb{R}^n : \langle a_i, x \rangle \leq b_i, i \in [m]\}$, we can define $M : \mathbb{R}^n \to \mathcal{S}^m$ via $M(x)_{ii} = b_i - \langle a_i, x \rangle$, for all $i \in [m]$ and $M(x)_{ij} = 0$ for $i \neq j$ and hence $Q = \{x \in \mathbb{R}^n : M(x) \in \mathcal{S}^m_+\}$. This shows that every polyhedron is a spectrahedron and therefore

$$\mathrm{sxc}(P) \leq \mathrm{xc}(P).$$

Hence, the upper bounds obtained in Sect. 3 also apply to the semidefinite case. Furthermore, it is clear from the definition that for any polyhedron P and any affine map π we have that $\mathrm{sxc}(\pi(P)) \leq \mathrm{sxc}(P)$. Moreover, Lemmas 2.1 and 2.2 analogously hold in the semidefinite case, since Yannakakis' result on the nonnegative rank of a slack matrix was extended to (PSD) lifts in [16, 22]: The semidefinite extension complexity P equals the *PSD rank* of S, which is the smallest dimension r for which there exist PSD matrices $F_1, F_2, \ldots, F_m \in \mathcal{S}^r_+$ and $V_1, V_2, \ldots, V_n \in \mathcal{S}^r_+$ such that $S_{ij} = \langle F_i, V_j \rangle$ where the scalar product of two matrices is defined via $\langle A, B \rangle = \sum_{i,j} A_{ij} B_{ij}$.

We obtain a superpolynomial lower bound on the semidefinite extension complexity of Voronoi cells of certain lattices using a lower bound of Lee et al. [32] on semidefinite extension complexities of correlation polytopes.

Theorem 5.1 *There exists a family of d-dimensional lattices Λ such that* $\mathrm{sxc}(\mathrm{VC}(\Lambda)) = 2^{\Omega(d^{1/13})}$.

Proof In [32] it is proven that the semidefinite extension complexity of the *correlation polytope*

$$P_n = \mathrm{conv}\,\{xx^\mathsf{T} : x \in \{0, 1\}^n\}$$

is bounded from below by $2^{\Omega(n^{2/13})}$. Notice that

$$P_n = \mathrm{conv}\,\{Y \in \{0, 1\}^{n \times n} : Y_{ij} \leq Y_{ii}, \ Y_{ij} \leq Y_{jj}, \ Y_{ii} + Y_{jj} - 1 \leq Y_{ij},$$
$$\text{for all } i, j \in [n] \text{ with } i \neq j\}.$$

Hence, the correlation polytope can be written as the convex hull of binary vectors $Y \in \{0, 1\}^{n \times n}$ satisfying linear inequalities whose slacks only have values in $\{0, 1\}$. Therefore, by Lemma 4.2 there is a lattice of dimension d where $d \leq n^2 + 1 = \Theta(n^2)$ such that P_n is a linear projection of a face F of $\mathrm{VC}(\Lambda)^\circ$. Analogously to the proof of Theorem 1.2 for the linear extension complexity, we conclude

$$\mathrm{sxc}(\mathrm{VC}(\Lambda)) = \mathrm{sxc}(\mathrm{VC}(\Lambda)^\circ) \geq \mathrm{sxc}(F) \geq \mathrm{sxc}(P_n) = 2^{\Omega(n^{2/13})},$$

and the claim follows since $n = \Omega(\sqrt{d})$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

6 Open Questions

We conclude our investigations of the extension complexity of Voronoi cells of lattices with a collection of some open problems that naturally arise from our studies and which we find interesting to pursue in future research.

In view of Theorem 1.2 a natural question is whether the logarithmic term in the lower bound $2^{\Omega(d/\log d)}$ on the extension complexity of certain Voronoi cells can be removed:

Question 6.1 *Does there exist a family of d-dimensional lattices Λ such that* $\mathrm{xc}(\mathrm{VC}(\Lambda)) = 2^{\Omega(d)}$?

We remark that our bound relies on a lower bound by Göös et al. [21] on extension complexities of stable set polytopes, which meet the criteria of Lemma 4.2. It is known that there *exist d*-dimensional 0/1-polytopes with extension complexity $2^{\Omega(d)}$, see [41]. However, no explicit construction of such polytopes is known and so it is unclear how to transform such polytopes in order to apply Lemma 4.1 efficiently.

Comparing the superpolynomial bound in Theorem 1.2 with the polynomial upper bounds for certain classes of lattices in Sect. 3, the question arises what we can expect the extension complexity of the Voronoi cell of a *generic* lattice to be.

Question 6.2 *What is* $\mathrm{xc}(\mathrm{VC}(\Lambda))$ *for a "random" d-dimensional lattice Λ?*

Of course, this requires a suitable notion of a random lattice. Our question refers to interesting examples such as Siegel's measure [45] or uniform distributions over integer lattices of a fixed determinant, see Goldstein and Mayer [20].

In Theorem 1.2 we have shown that *exactly* describing a Voronoi cell of a lattice may require superpolynomial-size extended formulations. It would be interesting to understand how this situation changes if we allow approximations instead of exact descriptions, in particular in view of various results on the complexity of the approximate closest vector problem, see, e.g., Aharonov and Regev [1]. To this end, for $\alpha \geq 1$ we say that a polytope Q is an α-*approximation* of a polytope P, if $P \subseteq Q \subseteq \alpha P$.

Question 6.3 *What can be said about extension complexities of α-approximations of Voronoi cells of lattices?*

We have seen in Theorem 1.1 that not only the root lattices but also their dual lattices have polynomial extension complexity. Is that a general phenomenon?

Question 6.4 *Given a d-dimensional lattice Λ, is there a polynomial relationship between* $\mathrm{xc}(\mathrm{VC}(\Lambda))$ *and* $\mathrm{xc}(\mathrm{VC}(\Lambda^{\star}))$?

Given that in view of Theorem 3.5 zonotopal lattices admit lifts with quadratically many facets, and the fact that the closest vector problem on such lattices can be solved in polynomial time (see [35]), one might expect that small-sized lifts of the corresponding Voronoi cells can actually be constructed explicitly.

Question 6.5 *Given a basis of a d-dimensional zonotopal lattice Λ, is it possible to construct an explicit lift of* $\mathrm{VC}(\Lambda)$ *with polynomially many facets in polynomial time?*

Note that our arguments leading to Theorem 3.5 are not constructive.

As discussed in the introduction, a small lift for the Voronoi cell of a lattice gives an expected polynomial-time algorithm for the closest vector problem. Similarly, given a *c-compact basis* $b_1, \ldots, b_k$ of a lattice Λ, i.e.,

$$\mathcal{F}(\Lambda) \subseteq \left\{ \sum_{i=1}^{k} \lambda_i b_i : \lambda \in [-c, c]^k \cap \mathbb{Z}^k \right\},$$

one can adjust the algorithm of Micciancio and Voulgaris to obtain a polynomial-space algorithm for the closest vector problem with running time $(2c)^{\mathcal{O}(n)}$. This notion was introduced in [28]. In Sect. 3.3, we have shown that there are lattices that do not admit c-compact bases for constant c but whose Voronoi cells have small lifts. One may ask whether the converse holds as well, or, equivalently:

Question 6.6 *Given a d-dimensional lattice Λ and a c-compact basis of Λ, can* $\mathrm{xc}(\mathrm{VC}(\Lambda))$ *be bounded by a polynomial in d, for fixed c?*

References

1. Aharonov, D., Regev, O.: Lattice problems in NP ∩ coNP. J. ACM **52**(5), 749–765 (2005)
2. Aprile, M., Fiorini, S.: Regular matroids have polynomial extension complexity. Math. Oper. Res. **47**(1), 540–559 (2022)
3. Balas, E.: Disjunctive programming. Ann. Discrete Math. **5**, 3–51 (1979)
4. Birkhoff, G.: Tres observaciones sobre el algebra lineal. Univ. Nac. Tucuman Ser. A **5**, 147–154 (1946)
5. Bogomolov, Yu., Fiorini, S., Maksimenko, A., Pashkovich, K.: Small extended formulations for cyclic polytopes. Discrete Comput. Geom. **53**(4), 809–816 (2015)
6. Chan, S.O., Lee, J.R., Raghavendra, P., Steurer, D.: Approximate constraint satisfaction requires large LP relaxations. J. ACM **63**(4), # 34 (2016)
7. Conforti, M., Cornuéjols, G., Zambelli, G.: Extended formulations in combinatorial optimization. Ann. Oper. Res. **204**, 97–143 (2013)
8. Conforti, M., Fiorini, S., Huynh, T., Weltge, S.: Extended formulations for stable set polytopes of graphs without two disjoint odd cycles. In: 21st International Conference on Integer Programming and Combinatorial Optimization (London 2020). Lecture Notes in Computer Science, vol. 12125, pp. 104–116. Springer, Cham (2020)

9. Conway, J.H., Sloane, N.J.A.: Sphere Packings, Lattices and Groups. Grundlehren der Mathematischen Wissenschaften, vol. 290. Springer, New York (1999)

10. Dadush, D., Bonifas, N.: Short paths on the Voronoi graph and closest vector problem with preprocessing. In: 26th Annual ACM-SIAM Symposium on Discrete Algorithms (San Diego 2015), pp. 295–314. SIAM, Philadelphia (2015)

11. van Emde Boas, P.: Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical report, Department of Mathematics, University of Amsterdam (1981)

12. Engel, P., Michel, L., Sénéchal, M.: Lattice Geometry (2004). https://cds.cern.ch/record/859509/files/cer-002542451.pdf

13. Erdahl, R.M.: Zonotopes, dicings, and Voronoi's conjecture on parallelohedra. Eur. J. Combin. **20**(6), 527–549 (1999)

14. Faenza, Y., Oriolo, G., Stauffer, G.: Separating stable sets in claw-free graphs via Padberg–Rao and compact linear programs. In: 23rd Annual ACM-SIAM Symposium on Discrete Algorithms (Kyoto 2012), pp. 1298–1308. ACM, New York (2012)

15. Fiorini, S., Kaibel, V., Pashkovich, K., Theis, D.O.: Combinatorial bounds on nonnegative rank and extended formulations. Discrete Math. **313**(1), 67–83 (2013)

16. Fiorini, S., Massar, S., Pokutta, S., Tiwary, H.R., de Wolf, R.: Linear vs. semidefinite extended formulations: exponential separation and strong lower bounds. In: 44th Annual ACM Symposium on Theory of Computing (New York 2012), pp. 95–106. ACM, New York (2012)

17. Fiorini, S., Massar, S., Pokutta, S., Tiwary, H.R., de Wolf, R.: Exponential lower bounds for polytopes in combinatorial optimization. J. ACM **62**(2), # 17 (2015)

18. Gerards, A.M.H.: Compact systems for T-join and perfect matching polyhedra of graphs with bounded genus. Oper. Res. Lett. **10**(7), 377–382 (1991)

19. Goemans, M.X.: Smallest compact formulation for the permutahedron. Math. Program. **153**(1), 5–11 (2015)

20. Goldstein, D., Mayer, A.: On the equidistribution of Hecke points. Forum Math. **15**(2), 165–189 (2003)

21. Göös, M., Jain, R., Watson, Th.: Extension complexity of independent set polytopes. SIAM J. Comput. **47**(1), 241–269 (2018)

22. Gouveia, J., Parrilo, P.A., Thomas, R.R.: Lifts of convex sets and cone factorizations. Math. Oper. Res. **38**(2), 248–264 (2013)

23. Grande, F., Padrol, A., Sanyal, R.: Extension complexity and realization spaces of hypersimplices. Discrete Comput. Geom. **59**(3), 621–642 (2018)

24. Grötschel, M., Lovász, L., Schrijver, A.: Geometric Algorithms and Combinatorial Optimization. Algorithms and Combinatorics, vol. 2. Springer, Berlin (1993)

25. Gruber, P.M.: Convex and Discrete Geometry. Grundlehren der Mathematischen Wissenschaften, vol. 336. Springer, Berlin (2007)

26. Heller, I.: On linear systems with integral valued solutions. Pac. J. Math. **7**(3), 1351–1364 (1957)

27. Hunkenschröder, Ch.: New Results in Integer and Lattice Programming. PhD thesis, EPFL, Lausanne (2020). https://www.epfl.ch/labs/disopt/wp-content/uploads/2020/06/hunkensc-diss.pdf

28. Hunkenschröder, Ch., Reuland, G., Schymura, M.: On compact representations of Voronoi cells of lattices. Math. Program. **183**, 337–358 (2020)

29. Kaibel, V., Weltge, S.: A short proof that the extension complexity of the correlation polytope grows exponentially. Discrete Comput. Geom. **53**(2), 397–401 (2015)

30. Kannan, R.: Minkowski's convex body theorem and integer programming. Math. Oper. Res. **12**(3), 415–440 (1987)

31. Korkine, A., Zolotareff, G.: Sur les formes quadratiques positives. Math. Ann. **11**(2), 242–292 (1877)

32. Lee, J.R., Raghavendra, P., Steurer, D.: Lower bounds on the size of semidefinite programming relaxations. In: 47th Annual ACM Symposium on Theory of Computing (Portland 2015), pp. 567–576. ACM, New York (2015)

33. Martin, R.K.: Using separation algorithms to generate mixed integer model reformulations. Oper. Res. Lett. **10**(3), 119–128 (1991)

34. Martinet, J.: Perfect Lattices in Euclidean Spaces. Grundlehren der Mathematischen Wissenschaften, vol. 327. Springer, Berlin (2003)

35. McCormick, S.Th., Peis, B., Scheidweiler, R., Vallentin, F.: A polynomial time algorithm for solving the closest vector problem in zonotopal lattices. SIAM J. Discrete Math. **35**(4), 2345–2356 (2021)

36. 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)

37. Moody, R.V., Patera, J.: Voronoi and Delaunay cells of root lattices: classification of their faces and facets by Coxeter–Dynkin diagrams. J. Phys. A **25**(19), 5089–5134 (1992)

38. von Neumann, J.: A certain zero-sum two-person game equivalent to the optimal assignment problem. In: Contributions to the Theory of Games, vol. 2. Annals of Mathematics Studies, vol. 28, pp. 5–12. Princeton University Press, Princeton (1953)

39. Pulleyblank, W.R., Shepherd, F.B.: Formulations for the stable set polytope of a claw-free graph. In: 3rd International Conference on Integer Programming and Combinatorial Optimization (Erice 1993), pp. 267–279. CIACO, Louvain-la-Neuve (1993)

40. Rajan, D.S., Shende, A.M.: A characterization of root lattices. Discrete Math. **161**(1–3), 309–314 (1996)

41. Rothvoß, Th.: Some 0/1 polytopes need exponential size extended formulations. Math. Progr. **142**(1–2), 255–268 (2013)

42. Rothvoss, Th.: The matching polytope has exponential extension complexity. J. ACM **64**(6), # 41 (2017)

43. Schürmann, A.: Computational Geometry of Positive Definite Quadratic Forms. Polyhedral Reduction Theories, Algorithms, and Applications. University Lecture Series, vol. 48. American Mathematical Society, Providence (2009)

44. Shitov, Ya.: Sublinear extensions of polygons (2014). arXiv:1412.0728

45. Siegel, C.L.: A mean value theorem in geometry of numbers. Ann. Math. **46**, 340–347 (1945)

46. Weltge, S.: Sizes of Linear Descriptions in Combinatorial Optimization. PhD thesis, Otto-von-Guericke-Universität Magdeburg (2015). https://doi.org/10.25673/4350

47. Wong, R.T.: Integer programming formulations of the traveling salesman problem. In: 1st IEEE International Conference on Circuits and Computers (Port Chester 1980), pp. 149–152. IEEE Press, Piscataway (1980)

48. Yannakakis, M.: Expressing combinatorial optimization problems by linear programs. J. Comput. Syst. Sci. **43**(3), 441–466 (1991)