

An upper bound on the number of perfect quadratic forms

W.P.J. van Woerden

Cryptography Group, CWI, Amsterdam, The Netherlands

Abstract

In a recent publication Roland Bacher showed that the number p_d of non-similar perfect d -dimensional quadratic forms satisfies $e^{\Omega(d)} < p_d < e^{O(d^3 \log(d))}$. We improve the upper bound to $e^{O(d^2 \log(d))}$ by a volumetric argument based on Voronoi's first reduction theory.

Keywords: Perfect quadratic form, Perfect lattice

2010 MSC: 11H55, 05E18

1. Introduction

The sphere packing problem is a classical problem with connections to fields of mathematics, information theory and physics. This problem asks how to pack d -dimensional identical balls in \mathbb{R}^d such that their density, the proportion of \mathbb{R}^d they fill, is maximized. All best known sphere packings up to dimension 9 are in fact lattice packings, i.e. sphere packings such that the centers of the balls form a discrete additive group. Therefore a natural restriction of the sphere packing problem is the lattice packing problem. In 1908, in his famous work [1], Voronoi introduced an algorithm that solves the lattice packing problem in any dimension in finite time. Voronoi showed that any lattice with optimal packing density must correspond to a so-called perfect (quadratic) form and his algorithm enumerates the finitely many perfect forms up to similarity in a fixed dimension. However, the number of non-similar perfect forms grows super-exponentially in the dimension and as a result Voronoi's algorithm has only been completely executed up to

Email address: wvw@cwi.nl (W.P.J. van Woerden)

Supported by the ERC Advanced Grant 740972 (ALGSTRONGCRYPTO).

dimension 8 [2, 3, 4, 5]. The exact number of non-similar perfect forms from dimension 2 up to 8 is 1, 1, 2, 3, 7, 33 and 10916 respectively and in dimension 9 more than 20 million were found [6]. An intriguing question is to characterize the growth of the number of non-similar perfect forms.

A bound on the number of perfect forms has consequences beyond estimating the complexity of Voronoi's algorithm. In 1998 C. Soulé [7] proved an upper bound of $e^{O(d^4 \log(d))}$, which he used to prove a statement related to Vandiver's Conjecture.

Furthermore, from the field of physics, there is interest in the statistical analysis of variations of Voronoi's algorithm based on random walks, first introduced by A. Andrianov and A. Scardicchio [8]. They conjecture a growth of $e^{\Theta(d^2)}$ and several variations of Voronoi's algorithm are designed [8, 9] under the assumption that this conjecture is true.

Recently R. Bacher [10] proved a lower bound of $e^{\Omega(d)}$ and an upper bound of $e^{O(d^3 \log(d))}$. Bacher already conjectured our improved upper bound of $e^{O(d^2 \log(d))}$ substantiated by heuristic arguments. However his proof methods and heuristic arguments do not seem to overlap with the proof we state here.

A useful property of d -dimensional perfect forms is that each of them has a corresponding full rank cone inside the cone of d -dimensional positive semidefinite quadratic forms. In fact if we look at all perfect forms up to scaling their corresponding cones are essentially disjoint. We use this property to prove the upper bound of $e^{O(d^2 \log(d))}$ with a volumetric argument. We show that each perfect form is similar to a perfect form of which the corresponding cone has at least a certain volume. As only a certain amount of such cones fit in a disjoint manner in the cone of positive semidefinite quadratic forms we obtain an upper bound on the number of similarity classes of perfect forms.

In Section 2 we discuss the preliminaries needed for the proof and in Section 3 we prove the upper bound of $e^{O(d^2 \log(d))}$.

2. Preliminaries

2.1. Notation

We denote the sets of integers, rationals and reals by \mathbb{Z} , \mathbb{Q} and \mathbb{R} respectively. With $\mathbb{R}_{\geq 0}$ and $\mathbb{R}_{> 0}$ we denote the set of all non-negative and positive reals respectively. The set of integers $\{1, 2, \dots, m\}$ is denoted by $[m]$ for any integer $m \geq 1$. A vector $v \in \mathbb{R}^d$ is interpreted as a single column matrix $v \in \mathbb{R}^{d \times 1}$. The i -th standard unit vector is denoted by $e_i \in \mathbb{Z}^d$. The transpose

of a vector $v \in \mathbb{R}^d$ or of a matrix $A \in \mathbb{R}^{d \times d}$ is denoted by v^t or A^t respectively. The standard inner product is often denoted by $v^t w = \sum_{i=1}^d v_i \cdot w_i \in \mathbb{R}$ and the outer product by $vw^t = (v_i \cdot w_j)_{i,j} \in \mathbb{R}^{d \times d}$ for vectors $v, w \in \mathbb{R}^d$. The trace and determinant of a square matrix A are denoted by $\text{Tr}(A)$ and $\det(A)$ respectively. The interior of a measurable set $S \subset \mathbb{R}^n$, i.e. the largest open set contained in S , is denoted by $\text{Int}(S)$. A cone is a set $C \subset \mathbb{R}^d$ that is closed under positive scaling. Let $X \subset \mathbb{R}^d$, then we denote by $\text{cone}(X)$ the cone given by all non-negative linear combinations of the elements in X and by $\text{conv}(X)$ the convex set given by all convex combinations of the elements in X . Furthermore we denote by $\text{rank}(X)$ the dimension of the linear subspace spanned by the elements in X .

2.2. Quadratic forms

We associate with every symmetric real matrix $Q \in \mathbb{R}^{d \times d}$ a (real) *quadratic form* in $d \geq 1$ variables given by

$$\begin{aligned} Q : \mathbb{R}^d &\rightarrow \mathbb{R}, \\ x &\mapsto Q[x] := x^t Q x. \end{aligned}$$

Remark that $Q[x] = Q[-x]$ for all $x \in \mathbb{R}^d$. The *space of all quadratic forms* is denoted by

$$\mathcal{S}^d := \{Q \in \mathbb{R}^{d \times d} : Q^t = Q\}.$$

Note that \mathcal{S}^d is an $n := \binom{d+1}{2}$ -dimensional real vector space, which is a Euclidean space when endowed with the standard *trace inner product*

$$\langle P, Q \rangle := \text{Tr}(P^t Q) = \sum_{i,j \in [d]} P_{ij} Q_{ij}.$$

The norm induced by this inner product is the standard Frobenius norm. By cyclicity of the trace, we have $x^t Q x = \langle Q, x x^t \rangle$. Under any fixed ordering of the indices $\{(i, j) \in [d] \times [d] : i \leq j\}$ a natural isometry ϕ from \mathcal{S}^d to the canonical Euclidean space \mathbb{R}^n is given by:

$$\phi : \mathcal{S}^d \rightarrow \mathbb{R}^n : Q \mapsto (q_{ij})_{i \leq j}$$

where $q_{ii} := Q_{ii}$ and $q_{ij} := \sqrt{2}Q_{ij} = \sqrt{2}Q_{ji}$ for $i < j$. Indeed we have

$$\langle \phi(P), \phi(Q) \rangle = \langle P, Q \rangle.$$

This isometry will implicitly be used in the figures. Moreover, we consider the *cone of positive definite quadratic forms* (PQFs)

$$\mathcal{S}_{>0}^d := \{Q \in \mathcal{S}^d : Q \text{ is positive definite}\},$$

its closure, the *cone of positive semidefinite quadratic forms*

$$\mathcal{S}_{\geq 0}^d := \{Q \in \mathcal{S}^d : Q \text{ is positive semidefinite}\},$$

and finally its historically named *rational closure* [11]

$$\tilde{\mathcal{S}}_{\geq 0}^d := \text{cone}(\{xx^t : x \in \mathbb{Z}^n\}) \subset \mathcal{S}_{\geq 0}^d.$$

2.3. Arithmetical equivalence

Two quadratic forms are *arithmetically equivalent* if they lie in the same orbit under the action $(Q, U) \mapsto U^t Q U$ of the multiplicative group

$$\text{GL}_d(\mathbb{Z}) := \{U \in \mathbb{Z}^{d \times d} : |\det U| = 1\}$$

of unimodular matrices. We call two PQFs $Q, Q' \in \mathcal{S}_{>0}^d$ *similar* if and only if Q is arithmetically equivalent to $\alpha Q'$ for some $\alpha \in \mathbb{R}_{>0}$.

2.4. Positive definite quadratic forms

For any PQF $Q \in \mathcal{S}_{>0}^d$ there exists a smallest real number $r > 0$ for which $Q[x] = r$ has an integral solution. We define this number as the *arithmetical minimum* denoted by

$$\lambda_1(Q) := \min_{x \in \mathbb{Z}^d \setminus \{0\}} Q[x].$$

More generally, we define for $i \in [d]$ the *i -th successive minima* $\lambda_i(Q)$ as

$$\begin{aligned} \lambda_i(Q) := \inf\{\lambda > 0 : \exists \mathbb{R}\text{-linearly independent } x_1, \dots, x_i \in \mathbb{Z}^n \setminus \{0\} \\ : Q[x_j] \leq \lambda \text{ for all } j \in [i]\}, \end{aligned}$$

where the infimum is in fact a minimum. Note that $\lambda_i(\alpha Q) = \alpha \lambda_i(Q)$ for any $\alpha \in \mathbb{R}_{>0}$. Furthermore, the successive minima are invariant under arithmetical equivalence, because $(U^t Q U)[x] = Q[Ux]$ and $U\mathbb{Z}^d = \mathbb{Z}^d$ for all $U \in \text{GL}_d(\mathbb{Z})$. So under the assumption that $\lambda_1(Q) = \lambda_1(Q')$ for two PQFs $Q, Q' \in \mathcal{S}_{>0}^d$, the notions of similarity and arithmetical equivalence coincide.

By applying Hermite-Korkine-Zolotarev lattice reduction to a PQF we can always find an arithmetically equivalent PQF for which the successive minima are attained, up to a factor linear in the dimension, by the standard basis of \mathbb{Z}^d .

Lemma 2.1 (Lagarias, Lenstra, Schnorr [12]). *Consider a PQF $Q \in \mathcal{S}_{>0}^d$. Then there exists a PQF $Q' \in \mathcal{S}_{>0}^d$ arithmetically equivalent to Q such that*

$$Q'[e_i] = Q'_{ii} \leq \frac{i+3}{4} \lambda_i(Q) \quad \text{for all } i \in [d].$$

We define the set of *minimal vectors* of a PQF $Q \in \mathcal{S}_{>0}^d$ as

$$\text{Min } Q := \{x \in \mathbb{Z}^d : Q[x] = \lambda_1(Q)\}.$$

Note that if $Q' = U^t Q U$, then $\text{Min } Q = U \cdot \text{Min } Q'$. We also define what is called the *Voronoi domain* $\mathcal{V}(Q)$ of a PQF $Q \in \mathcal{S}_{>0}^d$ as

$$\mathcal{V}(Q) := \text{cone}(\{xx^t : x \in \text{Min } Q\}) \subset \tilde{\mathcal{S}}_{\geq 0}^d.$$

A PQF $Q \in \mathcal{S}_{>0}^d$ is called *perfect* if the set of equations

$$\{Q'[x] = \lambda_1(Q) \text{ for all } x \in \text{Min } Q\},$$

has the unique solution $Q' = Q$ among $Q' \in \mathcal{S}^d$. That is, a perfect form is uniquely determined by its minimal vectors. Recall that $Q[x] = \langle Q, xx^t \rangle$, therefore a PQF $Q \in \mathcal{S}_{>0}^d$ is perfect if and only if its Voronoi domain $\mathcal{V}(Q)$ has full rank $n = \binom{d+1}{2}$ in \mathcal{S}^d . In particular any perfect form has at least n minimal vectors up to sign.

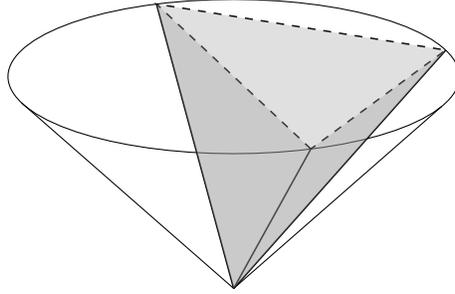


Figure 1: Voronoi domain of the perfect form $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ in the cone $\mathcal{S}_{\geq 0}^2$.

For a PQF $Q \in \mathcal{S}_{>0}^d$ we define the *dual* PQF as the inverse matrix $Q^{-1} \in \mathcal{S}_{>0}^d$; this coincides with lattice duality. Note that if the PQFs $Q, Q' \in \mathcal{S}_{>0}^d$ are arithmetically equivalent by U , then Q^{-1} and $(Q')^{-1}$ are arithmetically equivalent by U^{-t} . There are several metric relations between the PQFs Q and Q^{-1} , known as *transference theorems*. In particular for the successive minima we have bounds from Banaszczyk.

Theorem 2.2 (Banaszczyk [13, Thm. 2.1]). *Consider a PQF $Q \in \mathcal{S}_{>0}^d$. Then the successive minima of Q and its dual $Q^{-1} \in \mathcal{S}_{>0}^d$ satisfy*

$$\lambda_i(Q) \cdot \lambda_{d-i+1}(Q^{-1}) \leq d^2 \quad \text{for all } i \in [d].$$

2.5. Volume

By making use of the isometry $\phi : \mathcal{S}^d \rightarrow \mathbb{R}^n$ we only need the standard notion of volume in \mathbb{R}^n . The n -dimensional volume of a measurable set $S \subset \mathbb{R}^n$ of affine dimension at most n is denoted by $\text{Vol}_n(S)$. In particular the n -dimensional unit ball B^n has volume

$$\text{Vol}_n(B^n) = \frac{\pi^{n/2}}{\Gamma(n/2 + 1)},$$

where Γ denotes Euler's gamma function. Furthermore, a simplex, a convex set spanned by 0 and n linearly independent points $x_1, \dots, x_n \in \mathbb{R}^n$, has volume

$$\text{Vol}_n(\text{conv}\{0, x_1, \dots, x_n\}) = \frac{1}{n!} |\det((x_i)_{i \in [n]})|.$$

See [14] for a proof. If $S \subset \mathbb{R}^n$ is a convex measurable set of affine dimension $n - 1$ and $p \in \mathbb{R}^n$ is a point with orthogonal distance h to S , then it holds that

$$\text{Vol}_n(\text{conv}(S \cup \{p\})) = \frac{h}{n} \cdot \text{Vol}_{n-1}(S).$$

We call two measurable sets $S_1, S_2 \subset \mathbb{R}^n$ *essentially disjoint* if $\text{Int}(S_1) \cap \text{Int}(S_2) = \emptyset$. In particular for N pairwise essentially disjoint simplices $S_1, \dots, S_N \subset \mathbb{R}^n$ it holds that

$$\text{Vol}_n \left(\bigcup_{i=1}^N S_i \right) = \sum_{i=1}^N \text{Vol}_n(S_i).$$

3. An upper bound on the number of perfect forms

In this section we prove an upper bound on the number of non-similar d -dimensional perfect forms. The bound of $e^{O(d^2 \log(d))}$ improves on the bound of $e^{O(d^3 \log(d))}$ proven by R. Bacher [10]. Bacher already conjectured such an upper bound with heuristic arguments. Our proof strategy does not seem to overlap with the proof or the heuristic arguments of Bacher.

Theorem 3.1. *The number p_d of non-similar d -dimensional perfect quadratic forms has an upper bound of the form $e^{O(d^2 \log(d))}$. More precisely, p_d satisfies*

$$p_d \leq \frac{(n-1)!}{\Gamma(\frac{n}{2} + \frac{1}{2})} \cdot \sqrt{\frac{\pi^{n-1}}{2^{7n-d}}} \cdot \frac{(d-1)^{n-1}}{d^n} \cdot (d^3(d+7))^n, \quad \text{where } n = \binom{d+1}{2}.$$

The proof makes use of a volumetric argument after showing the existence of a good representative for each similarity class of perfect forms. Recall that every perfect form $Q \in \mathcal{S}_{>0}^d$ has a full rank Voronoi domain $\mathcal{V}(Q) = \text{cone}(\{xx^t : x \in \text{Min } Q\})$ in \mathcal{S}^d . A key point in the proof of Theorem 3.1 is that the Voronoi domains of the set of perfect forms up to scaling form an essentially disjoint partitioning of the rational closure $\tilde{\mathcal{S}}_{\geq 0}^d = \text{cone}\{xx^t : x \in \mathbb{Z}^n\}$.

Lemma 3.2 (Voronoi [1]). *The Voronoi domains of the d -dimensional perfect forms cover $\tilde{\mathcal{S}}_{\geq 0}^d$. Restricted to perfect forms $Q \in \mathcal{S}_{>0}^d$ with $\lambda_1(Q) = 1$, it holds that*

$$\tilde{\mathcal{S}}_{\geq 0}^d = \bigcup_{\substack{Q \text{ perfect} \\ \lambda_1(Q)=1}} \mathcal{V}(Q),$$

where the Voronoi domains are essentially disjoint.

Proof. This result originates from the first reduction theory of Voronoi [1], see section 7.1 of [15] for a full proof. We do reprove the last part of the Lemma, that is, the part that the union is essentially disjoint. This is the only part from this Lemma that we need. Let $Q, Q' \in \mathcal{S}_{>0}^d$ be two perfect forms where we assume that $\lambda_1(Q) = \lambda_1(Q') = 1$. Suppose that there exists an $R \in \text{Int}(\mathcal{V}(Q)) \cap \text{Int}(\mathcal{V}(Q'))$. We have to show that $Q = Q'$. Because $R \in \text{Int}(\mathcal{V}(Q))$, there exist positive $c_x \in \mathbb{R}_{>0}$ for every $x \in \text{Min } Q$ such that $R = \sum_{x \in \text{Min } Q} c_x \cdot xx^t$. As a result we have

$$\langle R, Q' \rangle = \sum_{x \in \text{Min } Q} c_x \cdot x^t Q' x \geq \sum_{x \in \text{Min } Q} c_x = \sum_{x \in \text{Min } Q} c_x \cdot x^t Q x = \langle R, Q \rangle,$$

using that $\lambda_1(Q) = \lambda_1(Q') = 1$. Because $R \in \text{Int}(\mathcal{V}(Q'))$ we get symmetrically the inequality $\langle R, Q' \rangle \leq \langle R, Q \rangle$ and thus equality. Then we have

$$0 = \langle R, Q' - Q \rangle = \sum_{x \in \text{Min } Q} c_x (x^t Q' x - 1).$$

Because $c_x > 0$ and $x^t Q' x \geq 1$ for all $x \in \text{Min } Q$, it holds that $x^t Q' x = 1$ for all $x \in \text{Min } Q$, i.e. $\text{Min } Q \subset \text{Min } Q'$. We conclude by perfectness of Q that $Q' = Q$. \square

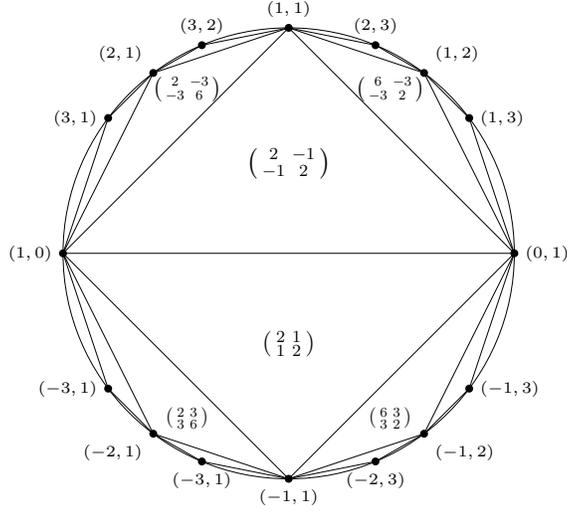


Figure 2: Partial partitioning of $\mathcal{S}_{\geq 0}^2$ by Voronoi domains viewed on a fixed trace plane. A vector x^t indicates the extreme ray xx^t . A matrix Q indicates the Voronoi domain $\mathcal{V}(Q)$.

To turn Lemma 3.2 into an upper bound on the number of non-similar perfect forms, we need to find, in each similarity class, a perfect form $Q \in \mathcal{S}_{>0}^d$ for which $\mathcal{V}(Q)$ is ‘large’. To find such a good representative we use the following lemma.

Lemma 3.3. *For all PQFs $Q \in \mathcal{S}_{>0}^d$, there exists a PQF $Q' \in \mathcal{S}_{>0}^d$ arithmetically equivalent to Q such that $x^t x \leq \frac{1}{8}d^3(d+7)$ for all $x \in \text{Min } Q'$.*

Proof. We can assume without loss of generality that $\lambda_1(Q) = 1$. Applying Lemma 2.1 to the dual PQF Q^{-1} we obtain a PQF $Q' \in \mathcal{S}_{>0}^d$ arithmetically equivalent to Q such that

$$(Q'^{-1})_{ii} \leq \frac{i+3}{4} \lambda_i(Q^{-1})$$

for all $i \in [d]$. Furthermore, note that $\lambda_d(Q) \geq \dots \geq \lambda_1(Q) = 1$ and thus by Theorem 2.2 we have

$$\lambda_i(Q^{-1}) \leq \frac{d^2}{\lambda_{d-i+1}(Q)} \leq d^2$$

for all $i \in [d]$. Combining these inequalities we obtain

$$\mathrm{Tr}(Q'^{-1}) = \sum_{i=1}^d (Q'^{-1})_{ii} \leq d^2 \cdot \sum_{i=1}^d \frac{i+3}{4} = \frac{1}{8}d^3(d+7).$$

In particular, this gives a lower bound on the eigenvalues $\mu_1, \dots, \mu_d > 0$ of Q' , namely

$$\frac{1}{\mu_i} \leq \sum_{j=1}^d \frac{1}{\mu_j} = \mathrm{Tr}(Q'^{-1}) \leq \frac{1}{8}d^3(d+7).$$

But as $\min_i \mu_i = \min_{y \in \mathbb{R}^d - 0} \frac{y^t Q' y}{y^t y}$ and $\lambda_1(Q') = \lambda_1(Q) = 1$ we have

$$x^t x \leq \frac{x^t Q' x}{\min_i \mu_i} \leq 1 \cdot \frac{1}{8}d^3(d+7)$$

for all $x \in \mathrm{Min} Q'$. □

To quantify the volume of the cones in $\mathcal{S}_{\geq 0}^d$, we bound them by the half-space $T_d = \{Q \in \mathcal{S}^d : \langle Q, I_d \rangle = \mathrm{Tr}(Q) \leq 1\}$ in \mathcal{S}^d . Recall the isometry $\phi : \mathcal{S}^d \rightarrow \mathbb{R}^n$ from Section 2.2. By Lemma 3.3, we can obtain for any similarity class a perfect form for which the Voronoi domain is reasonably large.

Corollary 3.4. *Consider a perfect quadratic form $Q \in \mathcal{S}_{> 0}^d$. Then there exists a perfect form $Q' \in \mathcal{S}_{> 0}^d$ arithmetically equivalent to Q such that*

$$\mathrm{Vol}_n(\phi(\mathcal{V}(Q') \cap T_d)) \geq \frac{1}{n!} \frac{2^{(n-d)/2}}{(\frac{1}{8}d^3(d+7))^n} =: \ell_d.$$

Proof. According to Lemma 3.3, there exists a PQF $Q' \in \mathcal{S}_{> 0}^d$ arithmetically equivalent to Q that satisfies $x^t x \leq \frac{1}{8}d^3(d+7)$ for all $x \in \mathrm{Min} Q'$. The

polytope $V' = \phi(\mathcal{V}(Q') \cap T_d)$ is the convex hull of 0 and $\phi\left(\frac{xx^t}{x^t x}\right)$ for all $x \in \text{Min } Q' / \{\pm 1\}$. As we are only in search of a lower bound for the volume of V' , we consider without loss of generality a subset $M_{Q'} \subset \text{Min } Q'$ such that $|M_{Q'}| = n$ and $\text{rank}\{\phi(xx^t) \in \mathbb{R}^n : x \in M_{Q'}\} = n$. Note that this is possible exactly because Q' is perfect. Then V' contains a simplex induced by $M_{Q'}$ and we get

$$\text{Vol}_n(V') \geq \text{Vol}_n\left(\text{conv}\left(\{0\} \cup \left\{\phi\left(\frac{xx^t}{x^t x}\right) : x \in M_{Q'}\right\}\right)\right) = \frac{1}{n!} |\det(W)|$$

with

$$W = \left(\phi\left(\frac{xx^t}{x^t x}\right)\right)_{x \in M_{Q'}} \in \mathbb{R}^{n \times n}.$$

By using that $\phi(xx^t) \in \mathbb{Z}^d \oplus \sqrt{2}\mathbb{Z}^{n-d}$ for all $x \in \mathbb{Z}^d$ under some fixed ordering and that the determinant of W is nonzero, because it has full rank, we get

$$\begin{aligned} |\det(W)| &= \left(\prod_{x \in M_{Q'}} \frac{1}{x^t x}\right) \cdot |\det((\phi(xx^t))_{x \in M_{Q'}})| \\ &\geq \left(\prod_{x \in M_{Q'}} \frac{1}{x^t x}\right) \cdot 2^{(n-d)/2} \geq \frac{2^{(n-d)/2}}{\left(\frac{1}{8}d^3(d+7)\right)^n}. \end{aligned}$$

So we can conclude that

$$\text{Vol}_n(\phi(\mathcal{V}(Q') \cap T_d)) \geq \frac{1}{n!} \cdot \frac{2^{(n-d)/2}}{\left(\frac{1}{8}d^3(d+7)\right)^n}.$$

□

Now we have found a good representative for each similarity class of perfect forms; the upper bound quickly follows.

Proof of Theorem 3.1. Let P_d be a complete set of non-equivalent representatives of perfect d -dimensional quadratic forms with $\lambda_1(Q) = 1$ up to arithmetical equivalence. By Corollary 3.4 we can assume that $\text{Vol}_n(\phi(\mathcal{V}(Q) \cap T_d)) \geq \ell_d$ for all $Q \in P_d$. By Lemma 1 we have

$$\bigcup_{Q \in P_d} \mathcal{V}(Q) \subset \tilde{\mathcal{S}}_{\geq 0}^d \subset \mathcal{S}_{\geq 0}^d,$$

where the $\mathcal{V}(Q)$ are essentially disjoint. This yields

$$|P_d| \cdot \ell_d \leq \sum_{Q \in P_d} \text{Vol}_n(\phi(\mathcal{V}(Q) \cap T_d)) \leq \text{Vol}_n(\phi(\mathcal{S}_{\geq 0}^d \cap T_d)).$$

What remains is to find an upper bound for the volume of $\mathcal{S}_{\geq 0}^d \cap T_d$. Remark that $\mathcal{S}_{\geq 0}^d \cap T_d$ is the convex hull of $0 \in \mathcal{S}^d$ and the convex base $C_d = \mathcal{S}_{\geq 0}^d \cap \{Q \in \mathcal{S}^d : \text{Tr}(Q) = 1\}$. Furthermore 0 has orthogonal distance $\|\frac{1}{d}I_d\|_F = \frac{1}{\sqrt{d}}$ to C_d . For $A = (a_{ij})_{i,j} \in C_d$ we have $a_{ij}^2 \leq a_{ii}a_{jj}$ for all $i, j \in [d]$, because A is positive semidefinite. Therefore, for any $A \in C_d$ we have

$$\langle A, A \rangle = \sum_{i,j \in [d]} a_{ij}^2 \leq \sum_{i,j \in [d]} a_{ii}a_{jj} = \text{Tr}(A)^2 = 1.$$

But then

$$\left\langle A - \frac{1}{d}I_d, A - \frac{1}{d}I_d \right\rangle = \langle A, A \rangle - \frac{2}{d} \text{Tr}(A) + \frac{1}{d} \leq \frac{d-1}{d},$$

and thus C_d is contained in an $(n-1)$ -dimensional ball with center $\frac{1}{d}I_d$ and radius $\sqrt{\frac{d-1}{d}}$. This implies the following upper bound.

$$\begin{aligned} \text{Vol}_n(\phi(\mathcal{S}_{\geq 0}^d \cap T_d)) &\leq \text{Vol}_n(\phi(\text{conv}(C_d \cup \{0\}))) \\ &= \frac{1}{n} \cdot \frac{1}{\sqrt{d}} \cdot \left(\frac{d-1}{d}\right)^{\frac{n-1}{2}} \cdot \text{Vol}_{n-1}(B^{n-1}) =: u_d. \end{aligned}$$

Recall that $n = \binom{d+1}{2} = O(d^2)$ and $n! \leq n^n = e^{O(d^2 \log(d))}$. To conclude,

$$|P_d| \leq \frac{u_d}{\ell_d} = \frac{(n-1)!}{\Gamma(\frac{n}{2} + \frac{1}{2})} \cdot \sqrt{\frac{\pi^{n-1}}{2^{7n-d}}} \cdot \frac{(d-1)^{n-1}}{d^n} \cdot (d^3(d+7))^n = e^{O(d^2 \log d)}.$$

□

4. An upper bound on the arithmetical minimum of perfect forms

We are grateful for the anonymous reviewer that suggested an additional remark, namely that Lemma 3.3 also results in an explicit upper bound on the arithmetical minimum $\lambda_1(Q)$ of a primitive integral perfect form Q . We denote the lattice of integral symmetric matrices by $\mathcal{S}^d(\mathbb{Z}) \subset \mathcal{S}^d$.

Theorem 4.1. *Let $Q \in \mathcal{S}_{>0}^d(\mathbb{Z})$ be a primitive and integral perfect form, then the arithmetical minimum $\lambda_1(Q)$ satisfies*

$$\lambda_1(Q) \leq 2^{-(n+d/2)} \cdot (d^3(d+7))^{n/2}, \text{ where } n = \binom{d+1}{2}.$$

Proof. By Lemma 3.3 we can assume that Q has n minimal vectors $x_1, \dots, x_n \in \mathbb{Z}^d$ with $x_i^t x_i \leq \frac{1}{8}d^3(d+7)$ that define a full rank system

$$\langle x_i x_i^t, Q' \rangle = \lambda_1(Q) \text{ for all } i \in [n],$$

with the unique solution $Q' = Q$. This translates to an integral linear system

$$A \cdot (Q'_{ij})_{i \leq j} = \lambda_1(Q) \cdot \mathbf{1}^n \quad \text{with } A := (\phi'(x_i x_i^t))_{i \in [n]} \in \mathbb{Z}^{n \times n},$$

using the embedding

$$\phi' : \mathcal{S}^d(\mathbb{Z}) \rightarrow \mathbb{Z}^d \oplus 2\mathbb{Z}^{n-d} : P \mapsto (p_{ij})_{i \leq j},$$

where $p_{ii} := P_{ii}$ and $p_{ij} := 2P_{ij}$ for $i < j$. This allows us to express Q as

$$(Q_{ij})_{i \leq j} = \frac{\lambda_1(Q)}{\det(A)} \cdot \text{adj}(A) \cdot \mathbf{1}^n \in \mathbb{Z}^n.$$

The adjugate $\text{adj}(A)$ of an integral matrix is integral and thus $\frac{\det(A)}{\lambda_1(Q)} \cdot Q$ is integral. As Q is primitive we get that $\lambda_1(Q) \leq \det(A)$ and we conclude by applying the Hadamard inequality as follows:

$$\begin{aligned} \det(A) &= \det(\phi'(x_i x_i^t))_{i \in [n]} = 2^{(n-d)/2} \cdot \det((\phi(x_i x_i^t))_{i \in [n]}) \\ &\leq 2^{(n-d)/2} \cdot \prod_{i=1}^n \|\phi(x_i x_i^t)\| \leq 2^{(n-d)/2} \cdot \left(\frac{1}{8}d^3(d+7)\right)^{n/2} \leq e^{O(d^2 \log d)}. \end{aligned}$$

□

References

- [1] G. Voronoï, Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Deuxième mémoire. Recherches sur les paralléloèdres primitifs., Journal für die reine und angewandte Mathematik 134 (1908) 198–287.

- [2] A. Korkine, G. Zolotareff, Sur les formes quadratiques, *Mathematische Annalen* 6 (3) (1873) 366–389.
- [3] E. S. Barnes, The complete enumeration of extreme senary forms, *Phil. Trans. R. Soc. Lond. A* 249 (969) (1957) 461–506.
- [4] D. O. Jaquet-Chiffelle, Énumération complète des classes de formes parfaites en dimension 7, *Annales de l’Institut Fourier* 43 (1) (1993) 21–55.
- [5] M. Dutour Sikirić, A. Schürmann, F. Vallentin, Classification of eight-dimensional perfect forms, *Electronic Research Announcements of the American Mathematical Society* 13 (3) (2007) 21–32.
- [6] W. P. J. van Woerden, Perfect quadratic forms: an upper bound and challenges in enumeration, Master’s thesis, Leiden University, (2018).
- [7] C. Soulé, Perfect forms and the Vandiver conjecture, *Journal für die Reine und Angewandte Mathematik* 517 (1999) 209–222.
- [8] A. Andreanov, A. Scardicchio, Random perfect lattices and the sphere packing problem, *Physical Review E* 86 (4) (2012) 041117.
- [9] A. Andreanov, A. Scardicchio, S. Torquato, Extreme lattices: symmetries and decorrelation, *Journal of Statistical Mechanics: Theory and Experiment* 2016 (11) (2016) 113301.
- [10] R. Bacher, On the number of perfect lattices, *Journal de Théorie des Nombres de Bordeaux* 30 (3) (2018) 917–945.
- [11] Y. Namikawa, Toroidal compactification of Siegel spaces, Vol. 812, Springer, 2006.
- [12] J. C. Lagarias, H. W. Lenstra, C. P. Schnorr, Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice, *Combinatorica* 10 (4) (1990) 333–348.
- [13] W. Banaszczyk, New bounds in some transference theorems in the geometry of numbers, *Mathematische Annalen* 296 (1) (1993) 625–635.
- [14] P. Stein, A note on the volume of a simplex, *The American Mathematical Monthly* 73 (3) (1966) 299–301.

- [15] J. Martinet, *Perfect Lattices in Euclidean Spaces*, Grundlehren der mathematischen Wissenschaften, Springer Berlin Heidelberg, 2002.