CLASSIFICATION OF EIGHT-DIMENSIONAL PERFECT FORMS

MATHIEU DUTOUR SIKIRIĆ, ACHILL SCHÜRMANN, AND FRANK VALLENTIN

(Communicated by Robert Griess)

ABSTRACT. In this paper, we classify the perfect lattices in dimension 8. There are 10916 of them. Our classification heavily relies on exploiting symmetry in polyhedral computations. Here we describe algorithms making the classification possible.

1. INTRODUCTION

A *lattice* L is a rank d subgroup of $\mathbb{R}^d$. It is of the form $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_d$ for linearly independent $v_1, \ldots, v_d$, which are called a *lattice basis* of L. The determinant $\det L = |\det(v_1, \ldots, v_d)|$ is independent of the chosen basis. By B^d we denote the Euclidean unit ball.

The *packing radius* $\lambda(L)$ of L is defined as half of the minimum distance between distinct lattice points. We call $L + \lambda(L)B^d$ the *lattice packing defined by* L. The *packing density* of the lattice packing defined by L is $\lambda(L)^d \operatorname{vol}(B^d)/\det L$, the proportion of space covered by balls. The *lattice packing problem* consists in finding the lattices having highest packing density.

A quadratic form $q(x)$ over $\mathbb{R}^d$ is a function defined as $q(x) = {}^t x Q x$ with Q a real $(d \times d)$ symmetric matrix. The quadratic form q is called *positive definite* if the corresponding matrix Q is positive definite. We denote by $\mathcal{S}^d$ (resp. $\mathcal{S}^d_{>0}$) the set of symmetric matrices (resp. positive definite matrices). In this paper, we will identify forms with their symmetric matrices. Two matrices $A, B \in \mathcal{S}^d_{>0}$ are called *arithmetically equivalent* if there exists a $P \in \operatorname{GL}_d(\mathbb{Z})$ such that $B = {}^t P A P$. Denote by $\operatorname{Aut}(A)$ the *arithmetic automorphism group* of $A \in \mathcal{S}^d$, i.e., the group of all $P \in \operatorname{GL}_d(\mathbb{Z})$ such that $A = {}^t P A P$.

If one takes a basis $V = (v_1, \ldots, v_d)$ of a lattice L, then L can be reconstructed, up to orthogonal transformations, from the Gram matrix $G_V = (\langle v_i, v_j \rangle) \in \mathcal{S}^d_{>0}$ with $\langle\ ,\ \rangle$ being the standard scalar product on $\mathbb{R}^d$. Another basis V' of L corresponds to another Gram matrix $G_{V'}$, which is arithmetically equivalent to G_V.

In other words, isometry classes of lattices are in one-to-one correspondence with arithmetical equivalence classes of positive definite quadratic forms. For computations, it is preferable to use the language of positive definite quadratic forms, which we will do in the remaining of the paper. For more details on the correspondence between lattice properties and quadratic forms, see [Ma03, Chapter 1].

The *arithmetical minimum* of a positive definite form A is

$$\lambda(A) = \min_{v \in \mathbb{Z}^d - \{0\}} {}^t v A v.$$

The *Hermite invariant* of A is defined as $\gamma(A) = \frac{\lambda(A)}{(\det A)^{1/d}}$. The *packing density* of the lattice corresponding to A is $\sqrt{\gamma(A)^d \frac{\mathrm{vol}(B^d)}{2^d}}$, with $\mathrm{vol}(B^d)$ being the volume of the unit ball B^d. Hence, solving the lattice packing problem is equivalent to maximizing γ over $\mathcal{S}^d_{>0}$. Denote by $\gamma_d = \max_{A \in \mathcal{S}^d_{>0}} \gamma(A)$ the *Hermite constant* in dimension d.

The set of *shortest vectors* of A is

$$\mathrm{Min}(A) = \{v \in \mathbb{Z}^d \mid {}^t v A v = \lambda(A)\} .$$

The form A is called *perfect* if the equations

$${}^t v B v = \lambda(A) \text{ for every } v \in \mathrm{Min}(A)$$

have the unique solution $B = A$ among $B \in \mathcal{S}^d$. Perfect forms were introduced in [KoZo73], and studied by many authors, for example, in [KoZo77], [Vo08], [Co51], [Ry70] and [CoSl88]. See also [Zo99] and [Ma03].

A form A is called *eutactic* if there exist $\lambda_v > 0$ such that

$$A^{-1} = \sum_{v \in \mathrm{Min}(A)} \lambda_v v^t v .$$

A form A is called *extreme* if the Hermite invariant γ attains a local maximum at A. Voronoi proved (see [Vo08, § 17] and [Ma03, Theorem 3.4.6]) that a form is extreme if and only if it is perfect and eutactic.

Given a perfect form A, its *perfect domain* is the polyhedral cone

$$\mathrm{Dom}(A) = \left\{ \sum_{v \in \mathrm{Min}(A)} \lambda_v v^t v \mid \lambda_v \geq 0 \right\} .$$

Perfect domains form a face-to-face tessellation containing the cone $\mathcal{S}^d_{>0}$, i.e., every $Q \in \mathcal{S}^d_{>0}$ belongs to at least one perfect domain and the intersection of two perfect domains $\mathrm{Dom}_1, \mathrm{Dom}_2$ is a face of both. If two perfect forms A, B are arithmetically equivalent, i.e., $A = {}^t P B P$ for some $P \in \mathrm{GL}_d(\mathbb{Z})$, then $\mathrm{Dom}(A) = P \, \mathrm{Dom}(B) \, {}^t P$. Voronoi proved (see [Vo08, § 7] and [Ma03, Theorem 7.4.4]) that for every fixed dimension d, the number of arithmetical inequivalent perfect forms is finite. Note that, since perfect domains form a tessellation of $\mathcal{S}^d_{>0}$, their interest is larger than only sphere packing theory (see, for example, [AMRT75], [Sh05] and [So05]).

Since the group $\mathrm{GL}_d(\mathbb{Z})$ acts on the tessellation with perfect domains, this provides an algorithm for classifying all perfect forms in a fixed dimension. In particular, one can solve the lattice packing problem using this algorithm.

Perfect forms have been classified up to dimension 7: In [KoZo77] Korkine and Zolotarev obtained the classification of perfect forms up to dimension 5 without using Voronoi's algorithm. The classification of perfect forms in dimensions 6, 7 was done by Barnes (see [Ba57]) and Jaquet (see [Ja93]) using Voronoi's algorithm.

TABLE 1. Perfect forms up to dimension 8. In fact, the lattices realizing the maximum of γ are root lattices (see [CoSl98, Chapter 6] or [Ma03, Chapter 4])

dim.	number of perfect lattices	authors	absolute maximum of γ realized by	number of extreme lattices
2	1	[La73]	$A_2 = \text{hex}$	1
3	1	[Ga40]	$A_3 = \text{fcc}$	1
4	2	[KoZo72]	D_4	2
5	3	[KoZo77]	D_5	3
6	7	[Ba57]	E_6	6
7	33	[Ja93]	E_7	30
8	10916		E_8	2408

Theorem 1.1. *There are* 10916 *perfect forms in dimension* 8.

We prove the above theorem by implementing Voronoi's algorithm (see [La71]). This enumeration problem in dimension 8 was considered by Martinet and his school. In fact, after the work of Laïhem [La92], Baril [Ba96], Napias [Na96], and Batut and Martinet [BaMa05], a list of 10916 perfect forms was known, and our contribution consists in proving that this list is complete. One key step of the enumeration is to prove:

Theorem 1.2. *The polyhedral cone* $\mathrm{Dom}(Q_{E_8})$ *has* 25075566937584 *facets in* 83092 *orbits.*

A direct consequence of the enumeration is:

Theorem 1.3 (Conjecture 6.6.7 of [Ma03]). *Every perfect* 8*-dimensional lattice has a basis of minimal vectors.*

Using the face structure of the perfect domains we obtain:

Theorem 1.4. *The set of possible kissing numbers* $|\mathrm{Min}(A)|$ *for* $A \in \mathcal{S}^8_{>0}$ *is* $2\{1, \ldots, 58,\, 60,\, 63, \ldots, 71,\, 75,\, 120\}$.

Using Theorem 1.1, Riener [Ri06] classified all extreme lattices in dimension 8:

Theorem 1.5. *There are* 2408 *extreme lattices in dimension* 8.

Note that Mordell's inequality $\gamma_{d+1} \leq \gamma_d^{d/(d-1)}$ (for a proof see [Mo44], [Zo99, Section 2.3] and [Ma03, Section 2.3]) and the knowledge of γ_7 and E_8 yield the value of γ_8. The value of γ_8 was first computed by Blichfeldt in [Bl35]. The first proof that E_8 is the unique form realizing γ_8 is in [Ve80]. Another proof based on analyzing the equality case in Mordell's inequality can be found in [Ma03, Section 6.6]. A completely different, computer assisted proof is in [CoKu04]. Our classification gives a fourth proof for the fact that E_8 is the unique lattice attaining γ_8.

Basic algorithms necessary for implementing Voronoi's algorithm are explained in Section 2; in Section 3 some dual description algorithms used are explained. In Section 4 we explain specific implementation details and, in Section 5, some consequences of our computation.

2. Basic algorithms

2.1. **Notions from polyhedral combinatorics.** By the Farkas-Minkowski-Weyl Theorem (see e.g. [Sch86, Corollary 7.1a]) a *convex polyhedral cone* $\mathcal{C} \subseteq \mathbb{R}^m$ is defined either by a finite set of *generators* $\{v_1, \ldots, v_N\} \subseteq \mathbb{R}^m$ or by a finite set of linear functionals $\{f_1, \ldots, f_M\} \subseteq (\mathbb{R}^m)^*$:

$$\mathcal{C} = \left\{ \sum_{i=1}^N \lambda_i v_i \mid \lambda_i \geq 0 \right\} = \left\{ x \in \mathbb{R}^m \mid f_i(x) \geq 0 \right\}.$$

$\mathcal{C}$ is called *full-dimensional* if the only vector space containing it is $\mathbb{R}^m$; $\mathcal{C}$ is called *pointed* if no linear subspace of positive dimension is contained in it.

Let $\mathcal{C}$ be a full-dimensional pointed convex polyhedral cone in $\mathbb{R}^m$. Given $f \in (\mathbb{R}^m)^*$, the inequality $f(x) \geq 0$ is said to be *valid* for $\mathcal{C}$ if it holds for all $x \in \mathcal{C}$. A *face* of $\mathcal{C}$ is a pointed polyhedral cone $\{x \in \mathcal{C} \mid f(x) = 0\}$, where $f(x) \geq 0$ is a valid inequality.

A face of dimension 1 is called an *extreme ray* of $\mathcal{C}$; a face of dimension $m-1$ is called a *facet* of $\mathcal{C}$. The set of faces of $\mathcal{C}$ forms a partially ordered set under inclusion. We write $F \lhd G$ if $F \subset G$ and $\dim F = \dim G - 1$. Two extreme rays of $\mathcal{C}$ are said to be *adjacent* if they generate a two-dimensional face of $\mathcal{C}$. Two facets of $\mathcal{C}$ are said to be *adjacent* if their intersection has dimension $m-2$. Any $(m-2)$-dimensional face of $\mathcal{C}$ is called a *ridge* and it is the intersection of exactly two facets of $\mathcal{C}$.

Every minimal set of generators $\{v_1, \ldots, v_{N'}\}$ defining $\mathcal{C}$ has the property

$$\{\mathbb{R}_+ v_1, \ldots, \mathbb{R}_+ v_{N'}\} = \{e \mid e \text{ is an extreme ray of } \mathcal{C}\}.$$

Every minimal set of linear functionals $\{f_1, \ldots, f_{M'}\}$ defining $\mathcal{C}$ has the property that $\{F_1, \ldots, F_{M'}\}$ with $F_i = \{x \in \mathcal{C} \mid f_i(x) = 0\}$ is the set of facets of $\mathcal{C}$. The problem of transforming a minimal set of generators into a minimal set of linear functionals (or vice versa) is called the *dual description problem*.

2.2. **Voronoi's algorithm for classifying perfect forms.** In this section we describe Voronoi's algorithm. It computes a complete representative system of arithmetically inequivalent perfect forms:

Input: Dimension d.
Output: Set $\mathcal{M}$ of all inequivalent d-dimensional perfect forms.

$T \leftarrow \{Q_{\mathsf{A}_n}\}$.
$\mathcal{M} \leftarrow \emptyset$.
while there is a $Q \in T$ **do**
    $\mathcal{M} \leftarrow \mathcal{M} \cup \{Q\}$.
    $T \leftarrow T \setminus \{Q\}$.
    $\mathcal{F} \leftarrow$ facets of $\mathrm{Dom}(Q)$.
    for $F \in \mathcal{F}$ **do**
        find perfect form Q' with $F = \mathrm{Dom}(Q) \cap \mathrm{Dom}(Q')$.
        if Q' is not equivalent to a form in $\mathcal{M} \cup T$ **then**
            $T \leftarrow T \cup \{Q'\}$.
        end if
    end for
end while

For the quadratic form Q_{A_n} in the above algorithm, we may use $Q_{A_n} = (q_{i,j})_{1 \leq i,j \leq n}$ with $q_{i,i} = 2$, $q_{i,i-1} = q_{i-1,i} = -1$ and $q_{i,j} = 0$ otherwise (see [CoSl98, Section 6.1] or [Ma03, Section 4.2]).

By Voronoi's finiteness theorem, we know that the above program will eventually finish.

The dual description part, which is used in computing the facets of $\mathrm{Dom}(Q)$, is computationally the most demanding part. The special methods used for that purpose are explained in Section 3. The computation of the adjacent domain is explained in Section 2.3, and the test of isometry of lattices, in Section 2.4.

2.3. Adjacent domain and shortest vector problems.
In this section we describe the subalgorithm which computes the adjacent perfect domain. Given a positive definite form A we need to solve the shortest vector problem, i.e., compute its arithmetical minimum $\lambda(A)$ and the set of vectors $\mathrm{Min}(A)$ that realize it. The Fincke-Pohst algorithm (cf. [Co93, Algorithm 2.7.7]), which has many implementations (sv [Va99], in GAP, in MAGMA, in PARI, etc.), does this. In particular, solving a shortest vector problem in dimension 8 is a routine task and takes only a fraction of a second.

If F denotes a facet of $\mathrm{Dom}(A)$ with A a perfect form, then we define

$$\mathrm{Min}_F(A) = \{v \in \mathrm{Min}(A) \mid v^t v \in F\} .$$

We then have the following algorithm:

Input: Perfect form A and facet F of $\mathrm{Dom}(A)$.
Output: Perfect form A' with $\mathrm{Dom}(A') \cap \mathrm{Dom}(A) = F$.

$w \leftarrow$ an element of $\mathrm{Min}_F(A)$.
$U \leftarrow$ solution in $\mathcal{S}^d$ of $^t v U v = 0$ for $v \in \mathrm{Min}_F(A)$ and $^t v U v = 1$ for a
     $v \in \mathrm{Min}(A) - \mathrm{Min}_F(A)$.
$\lambda \leftarrow 1$.
while $\mathrm{Min}(A + \lambda U) \subset \mathrm{Min}(A)$ **do**
     $\lambda \leftarrow 2\lambda$.
end while
while there is a $v_0 \in \mathbb{Z}^n - \{0\}$ such that $^t v_0 (A + \lambda U) v_0 < {}^t w(A + \lambda U)w$ **do**
     $\lambda \leftarrow$ solution of $^t v_0 (A + \lambda U) v_0 = {}^t w(A + \lambda U)w$.
end while
$A' \leftarrow A + \lambda U$.

How do we test if there is a $v_0 \in \mathbb{Z}^n - \{0\}$ such that $^t v_0 A' v_0 < {}^t w A' w$? If A' is positive definite, this is done by solving a shortest vector problem. If A' is positive semidefinite but not positive definite, we can find a vector $v_0 \in \mathbb{Z}^n - \{0\}$ in the kernel of A', which will satisfy $^t v_0 A' v_0 = 0$. If A' is not definite, we can find a vector $v_0 \in \mathbb{Z}^n - \{0\}$ such that $^t v_0 A' v_0 \leq 0$ by taking rational approximations of an eigenvector corresponding to a negative eigenvalue.

Note that any $P \in \mathrm{Aut}(A)$ defines an action on $\mathrm{Min}(A)$ by $x \mapsto Px$. This makes the group $\mathrm{Aut}(A)$ act on $\mathrm{Min}(A)$, on the facets of $\mathrm{Dom}(A)$ and on the perfect domains adjacent to $\mathrm{Dom}(A)$.

2.4. Isometry tests.
In order to implement Voronoi's algorithm, we need to be able to decide if two perfect forms A and B are arithmetically equivalent or not. We also need, for the dual description algorithm explained later, a way to compute $\mathrm{Aut}(A)$.

If A and B are perfect forms, then $B = {}^tPAP$ if and only if $P\,\mathrm{Min}(A) = \mathrm{Min}(B)$. One implication is immediate; the other follows from the definition of perfect forms. Hence a possible algorithm is to compute $\mathrm{Min}(A)$ and $\mathrm{Min}(B)$ and search for a $P \in \mathrm{GL}_n(\mathbb{Z})$ such that $P\,\mathrm{Min}(A) = \mathrm{Min}(B)$; the search space is finite since $\mathrm{Min}(A)$ and $\mathrm{Min}(B)$ are finite and form a generating system of $\mathbb{R}^n$.

For a non-perfect form the set of minimal vectors does not characterize it. However, a form $A \in \mathcal{S}^d$ is uniquely characterized by the set of all vectors $v \in \mathbb{Z}^n$ with *norm* ${}^tvAv$ less or equal to the maximum diagonal coefficient $\max_{i=1}^d A_{i,i}$. The program `Isometry` (see [PlOpSc98], [PlSo97]), and its companion `Aut_Grp` for computing the automorphism group of a form, work by generating these possibly very large vector sets. Hence in order to speed up computations with these programs, it is desirable to compute with forms with small, maximum diagonal coefficients. This can be achieved by storing only a *Minkowski reduced form* for each equivalence class. Such can be obtained for example with the program `Mink_red` (see [PlOpSc98]).

3. Dual description methods

General purpose programs like `cdd` [Fu95], `lrs` [Av93], `pd` [Ma97], and `porta` [ChLo97] allow one to compute the dual description of a polyhedral cone given by its facets (linear inequalities) or by its extreme rays (generators). Since the programs are implementations of quite different methods, their efficiency may vary tremendously on a particular cone. The perfect form Q_{E_8} (see [CoSl98, Chapter 6]) has $|\mathrm{Min}(Q_{\mathsf{E}_8})| = 240$, and therefore the 36-dimensional cone $\mathrm{Dom}(Q_{\mathsf{E}_8})$ has 120 extreme rays. All general purpose programs take too much time in computing the facets of this cone.

Usually one is interested only in a list of representatives of orbits of facets and not in the full list of facets. This leads us naturally to the *Adjacency Decomposition Method*, which exploits the symmetry of a polyhedral cone. The programs mentioned above are still used, but as subroutines. In the following discussion, we will assume that $\mathcal{C}$ is a full-dimensional, pointed polyhedral cone in $\mathbb{R}^m$ generated by the extreme rays $(e_i)_{1 \le i \le N}$, and we want to compute its facets.

3.1. Adjacency Decomposition Method.

Input: Extreme rays of a polyhedral cone $\mathcal{C}$ and a group G acting on $\mathcal{C}$.
Output: Complete set $\mathcal{M}$ of inequivalent facets of $\mathcal{C}$ under G.

$T \leftarrow \{F\}$ with F a facet of $\mathcal{C}$.
$\mathcal{M} \leftarrow \emptyset$.
while there is a $F \in T$ **do**
$\quad \mathcal{M} \leftarrow \mathcal{M} \cup \{F\}$.
$\quad T \leftarrow T \setminus \{F\}$.
$\quad \mathcal{F} \leftarrow$ facets of F.
$\quad$ **for** $H \in \mathcal{F}$ **do**
$\quad\quad$ find facet F' of $\mathcal{C}$ with $H = F \cap F'$.
$\quad\quad$ **if** F' is not equivalent under G to a facet in $\mathcal{M} \cup T$ **then**
$\quad\quad\quad T \leftarrow T \cup \{F'\}$.
$\quad\quad$ **end if**
$\quad$ **end for**
end while

Note that Voronoi's algorithm is very similar to the Adjacency Decomposition Method. Both fit into the framework of *graph traversal algorithms*. In the above algorithm, an initial facet can be found by solving a linear program.

The algorithm relies on the ability to test if two facets are equivalent under the symmetry group. The possible strategies and the one that we used are explained in Section 4. The Adjacency Decomposition Method framework is a reasonably natural algorithm for computing with symmetry. Hence it was discovered several times, for example, in [Ja93] as "algorithm de l'explorateur", in [ChRe96] as "adjacency decomposition method", and in [DFPS01] as "subpolytope algorithm".

We explain here the *gift-wrapping step* (see [Swa85]) to compute an adjacent facet. Given the list of extreme rays $(e_i)_{1 \leq i \leq N}$, a facet $F \lhd \mathcal{C}$ is encoded by an index set $S_F \subset \{1, \ldots, N\}$ such that F is generated by $(e_i)_{i \in S_F}$. Given a ridge H, we need an algorithm for computing the uniquely determined facet F' of $\mathcal{C}$ such that $F \cap F' = H$. The ridge H is encoded by a set $S_H \subset S_F$ such that $(e_i)_{i \in S_H}$ generate H. The defining inequalities $f \in (\mathbb{R}^m)^*$ of the facet F' should satisfy $f(e_i) = 0$ for all $i \in S_H$. The vector space of such functions has dimension 2. Let us select a basis $\{f_1, f_2\}$ of it. If $f = \alpha_1 f_1 + \alpha_2 f_2$ is the defining inequality of F or F', $f(e_i) \geq 0$ for all i with $1 \leq i \leq N$. This translates into a set of linear inequalities on α_1, α_2 defining a 2-dimensional pointed polyhedral cone. One easily finds its two generators $(\alpha_1^i, \alpha_2^i)_{1 \leq i \leq 2}$. The corresponding inequalities $f_i(x) = \alpha_1^i f_1(x) + \alpha_2^i f_2(x) \geq 0$ on $\mathcal{C}$ define the two adjacent facets F and F' of $\mathcal{C}$.

The Adjacency Decomposition Method can find the dual description of very symmetric polyhedral cones, when other methods fail. But this algorithm uses dual description, albeit in one dimension lower and again this computation might be impossible by the known general purpose algorithms. The *incidence number* of a face is the number of extreme rays contained in it; from our experience it is a good measure of the complexity of a face: in all polyhedral cones encountered by us so far, the facets with the highest incidence number are the ones of highest symmetry and they are also the ones whose dual description is the most difficult to compute.

As a consequence, we begin the computation from the orbit with the lowest incidence number, since they are presumably easiest to treat and we may not need to treat all orbits, because of the following theorem due to Balinski:

Theorem 3.1 ([Ba61]; see e.g. [Zi95, Theorem 3.14])**.** *Let $\mathcal{C}$ be an m-dimensional, pointed polyhedral cone. Let G be the undirected graph whose vertices are the facets of $\mathcal{C}$ and whose edges are the ridges of $\mathcal{C}$. Two vertices E_1, E_2 are connected by an edge F if $E_1 \cap E_2 = F$. Then, the graph G is $(m-1)$-connected, i.e., removal of any $m-2$ vertices leaves it connected.*

Using the above theorem, we know that if the total number of facets in unfinished orbits is less than $m-1$, then they cannot be adjacent to yet to be discovered facets and so we are done. In practice this simple criterion, which can be regarded as an extension of Theorem 7 and its corollaries in [Ja93], is extremely useful and many difficult computations were finished by it.

3.2. **Recursive Adjacency Decomposition Method.** When there are only a few remaining facets to treat and we cannot apply Theorem 3.1, our method is to use the Adjacency Decomposition Method on the remaining untreated facets of $\mathcal{C}$ recursively. The problem is that one may be confronted with a lot of cases to

consider. In this section we present the method used to make this manageable in some cases.

If a face F' satisfies $F' \lhd F_1 \lhd \mathcal{C}$ for a facet F_1, then there is exactly one other facet F_2 such that $F' \lhd F_2 \lhd \mathcal{C}$. Hence, if one applies the Adjacency Decomposition Method to F_1 and F_2, then one will compute the dual description of F' two times. The number of such repetitions increases as the recursion depth increases.

To handle this, we use a *banking system*. We store the representatives of orbits of $(k-1)$-dimensional faces (facets) F of a k-face F' with respect to a group $\mathrm{Grp}_{F'} \subseteq \mathrm{Aut}_{F'}$ of linear automorphisms of F', which is not necessarily the full automorphism group of F'.

If $F' \lhd F''$ and the Adjacency Decomposition Method is applied to F'', then as a subtask one needs to find the orbits of facets of F' under the stabilizer $\mathrm{Stab}(\mathrm{Grp}_{F''}, F')$ of F' under the group $\mathrm{Grp}_{F''}$. So, the problem is to obtain the list of facets under the action of $\mathrm{Stab}(\mathrm{Grp}_{F''}, F')$ from a list of orbits under the action of $\mathrm{Grp}_{F'}$.

When $\mathrm{Stab}(\mathrm{Grp}_{F''}, F')$ is not a subgroup of $\mathrm{Grp}_{F'}$ (we did not require that $\mathrm{Grp}_{F'} = \mathrm{Aut}_{F'}$), then we replace $\mathrm{Grp}_{F'}$ by the group generated by $\mathrm{Grp}_{F'}$ and $\mathrm{Stab}(\mathrm{Grp}_{F''}, F')$. So, we can assume that $\mathrm{Stab}(\mathrm{Grp}_{F''}, F') \subseteq \mathrm{Grp}_{F'}$. Take an orbit $\mathrm{Grp}_{F'} F$ of $(k-1)$-dimensional faces of the k-dimensional face F'. We find elements $g_1, \ldots, g_r$ in $\mathrm{Grp}_{F'}$ such that

$$\mathrm{Grp}_{F'} = \bigcup_{i=1}^{r} \mathrm{Stab}(\mathrm{Grp}_{F''}, F') g_i \, \mathrm{Stab}(\mathrm{Grp}_{F'}, F),$$

i.e., we compute a decomposition of $\mathrm{Grp}_{F'}$ into *double cosets* (using a computer algebra system like `GAP` [GAP05]). One then obtains

$$\mathrm{Grp}_{F'} F = \bigcup_{i=1}^{r} \mathrm{Stab}(\mathrm{Grp}_{F''}, F') g_i F,$$

i.e., the orbit $\mathrm{Grp}_{F'} F$ splits into r orbits $\mathrm{Stab}(\mathrm{Grp}_{F''}, F') F_i$ with $F_i = g_i F$. This double coset decomposition is a classic enumeration technique, exposed for example in [Br00] and [Ke99].

To set up a banking system as described, we need to be able to test if two polyhedral cones are isomorphic and we need to compute their automorphism groups.

3.3. Isomorphisms and automorphisms of polyhedral cones.

The symmetry group of a pointed polyhedral full-dimensional cone in $\mathbb{R}^m$ generated by extreme rays $(e_i)_{1 \leq i \leq N}$ is the group of matrices $A \in \mathrm{GL}_m(\mathbb{R})$ such that there exists a permutation σ of $\{1, \ldots, N\}$ with $A e_i = e_{\sigma(i)}$ for $1 \leq i \leq N$. This infinite group is called a *projective automorphism group* (see [KaSc03]).

We are not aware of an algorithm to decide whether or not polyhedral cones are equivalent and to compute their projective automorphism groups. However, for the stronger notion of restricted equivalence introduced below, we can resolve those questions. Computing with a proper subgroup of the projective automorphism group is not a problem for the Recursive Adjacency Decomposition Method. However, it impacts the computing time since we may compute the dual description of projectively isomorphic polyhedral cones several times.

Given a full-dimensional vector family $(v_i)_{1 \leq i \leq N}$, we define the positive definite matrix

$$Q = \sum_{i=1}^{N} v_i \, {}^t v_i \in \mathcal{S}_{>0}^m \, .$$

Furthermore, denote by R the unique matrix $R \in \mathcal{S}_{>0}^m$ satisfying $Q^{-1} = R^2$, and $(w_i)_{1 \leq i \leq N} = (Rv_i)_{1 \leq i \leq N}$, the image of the family (v_i) under R. Define $G(v_i)$ to be the complete graph with vertices v_i and edge weights $c_{ij} = {}^t v_i Q^{-1} v_j = \langle w_i, w_j \rangle$.

A *restricted isomorphism* of two vector families $(v_i)_{1 \leq i \leq N}$ and $(v_i')_{1 \leq i \leq N}$ is given by a matrix A such that there exists a permutation σ satisfying $Av_i = v_{\sigma(i)}'$ for $i = 1, \ldots, N$.

Such a restricted isomorphism satisfies $AQ^t A = Q'$ with Q and Q' as above. One then checks that the matrix $O = R'AR^{-1}$ is orthogonal and satisfies $Ow_i = w_{\sigma(i)}'$. This implies $c_{ij} = c_{\sigma(i)\sigma(j)}'$; i.e., the restricted isomorphism of the vector families (v_i) and (v_i') corresponds to an isomorphism between the edge weighted graphs $G(v_i)$ and $G(v_i')$.

Now we need to prove that if σ is an isomorphism between $G(v_i)$ and $G(v_i')$, then the equation $Av_i = v_{\sigma(i)}'$ admits only one solution. Clearly, we can assume $\sigma = \mathrm{Id}$ and consider the equivalent equation $Ow_i = w_i'$. Since the v_i generate $\mathbb{R}^m$, we find a basis $(v_{i_1}, \ldots, v_{i_m})$ of $\mathbb{R}^m$. If P, respectively P', is the $m \times m$ matrix formed by (w_{i_k}), respectively (w_{i_k}'), then the equation $c_{ij} = c_{ij}'$ takes the form ${}^t PP = {}^t P'P'$. So, the matrix $O = P'P^{-1}$ is orthogonal and one has for any $1 \leq k \leq m$, $1 \leq j \leq N$:

$$\langle w_{i_k}', Ow_j \rangle = \langle Ow_{i_k}, Ow_j \rangle = \langle w_{i_k}, w_j \rangle = \langle w_{i_k}', w_j' \rangle.$$

The above equation gives $\langle w_i', Ow_j - w_j' \rangle = 0$; since the w_i' form a basis of $\mathbb{R}^m$, we obtain the relation $Ow_j = w_j'$, i.e., a restricted isomorphism between (v_i) and (v_i'). In the same manner one proves that the restricted automorphism problem for a vector family $(v_i)_{1 \leq i \leq N}$ is equivalent to the automorphism problem of the edge weighted graph $G(v_i)$.

4. Implementation details

The key part of our algorithm is to test if two $(k-1)$-dimensional faces of a k-dimensional face F are equivalent under a group Grp_F of automorphisms of F. In practice, we represent $(k-1)$-dimensional faces by the set of indices of extreme rays contained in F and we use the command RepresentativeAction with the action OnSets of the GAP computer algebra system [GAP05] to test for equivalence. We compute the stabilizer of a face with the Stabilizer command. Building the full orbit, a strategy we could not consider, is used in [DFPS01] and [DeDu03]. For some special groups and representations, like $\mathrm{Sym}(n)$ acting on n elements, it is very easy to test equivalence; this strategy is used in [An03] and [ChRo99].

In practice, the program nauty [MKa05] computes efficiently isomorphisms and automorphisms for vertex weighted graphs. Its "User's Guide" (Version 2.4, page 25) contains a description of a simple method to transform edge weighted problems into vertex weighted ones.

5. Computational results

To compute the dual description of the 10916 perfect domains we only had to use the Adjacency Decomposition Method in two cases: for E_8 and for the Barnes-Coxeter lattice A_8^2 (cf. [Ma03, Section 5.1]). It would also be necessary for the lattice D_8 (cf. [Ja92]), but for D_n the list of neighboring domains is already known; see [RyBa79, Theorem 15]. All other domains could be treated by the standard software `lrs`.

Computing the dual description of $\mathrm{Dom}(Q_{\mathsf{E}_8})$ (its symmetry group is $W(E_8)/\mathbb{Z}_2$ of size 348364800) took several months of computer time.

Most of the time of this computation was used for treating three orbits of facets of $\mathrm{Dom}(Q_{\mathsf{E}_8})$ generated by 66, 70, and 75 extreme rays respectively. The facet with 75 extreme rays is interesting: its stabilizer under the action of the group $W(\mathsf{E}_8)/\mathbb{Z}_2$ has size 23040, but when the automorphism group is computed, the size grows to 737280, therefore allowing us to finish the computation. We have no theoretical explanation for those additional symmetries.

It is proved in [Wa71] that if a positive definite form A has $\frac{1}{2}|\mathrm{Min}(A)| > 75$, then A is arithmetically equivalent to a multiple of Q_{E_8}. The knowledge of facets of the perfect domain allows us to say a bit more: If $\frac{1}{2}|\mathrm{Min}(A)| = 75$, then $A = \lambda_1 A_1 + \lambda_2 A_2$ with both A_i arithmetically equivalent to Q_{E_8} and $\lambda_i > 0$. If $\frac{1}{2}|\mathrm{Min}(A)| = 70$, then $A = \lambda_1 A_1 + \lambda_2 A_2$ with $\lambda_i > 0$, A_1 arithmetically equivalent to Q_{E_8} and A_2 arithmetically equivalent to $Q_{\mathsf{A}_8^2}$.

It is also worthwhile to note that the form Q_{E_8} is not contiguous to only two forms: Q_{A_8} and the one with number 8190 (see `http://www.math.uni-magdeburg.de/lattice_geometry/` for the contiguities).

The method developed here allowed us to treat the 8-dimensional case. Without using symmetry of perfect domains, one would be limited to dimension 6. Note that the algorithm developed by Jaquet in [Ja93] for dimension 7 is also a Recursive Adjacency Decomposition Method; he does not use a banking system and instead of using a standard software for the double description (which did not exist at that time) he uses a specific "Cascade algorithm". We computed the facets of the perfect domain $\mathrm{Dom}(Q_{\mathsf{E}_7})$ in less than a day.

In dimension 9, a priori it seems currently very difficult to do a full computation of the list of perfect forms. Their number becomes even larger. We found more than 500000 (see `http://www.math.uni-magdeburg.de/lattice_geometry/`) and there is no end in sight. Nevertheless, it is probably only a matter of time until the perfect forms in dimension 9 can be enumerated by Voronoi's algorithm.

References

[An03]   M.M. Anzin, *On the density of a lattice covering for $n = 11$ and $n = 14$*, Tr. Mat. Inst. Steklova **239** (2002), Diskret. Geom. i Geom. Chisel, 20–51; translation in Proc. Steklov Inst. Math. **239-4** (2002) 13–44. MR1975133 (2004i:11066)

[AMRT75]   A. Ash, D. Mumford, M. Rapoport, and Y. Tai, *Smooth compactification of locally symmetric varieties*, Lie groups: History, Frontiers and Applications, Vol IV, Math. Sci. Press, Brookline, Mass., 1975. MR0457437 (56:15642)

[Av93]   D. Avis, *A C-implementation of the reverse search vertex enumeration algorithm*, School of Computer Science, McGill University, Montreal, Canada 1993, `http://www-cgrl.cs.mcgill.ca/~avis/C/lrs.html`.

[Ba61]   M.L. Balinski, *On the graph structure of convex polyhedra in n-space*, Pacific J. Math. **11** (1961) 431–434. MR0126765 (23:A4059)

[Ba96]   J-L. Baril, *Autour de l'algorithme de Voronoi: Construction de réseaux Euclidiens*, Thèse, Bordeaux (1996).

[Ba57]   E.S. Barnes, *The complete enumeration of extreme senary forms*, Phil. Trans. Roy. Soc. London **249-A** (1957) 461–506. MR0086833 (19:251d)

[BaMa05]   C. Batut and J. Martinet, *A catalogue of perfect lattices*, `http://www.math.u-bordeaux.fr/~martinet/`.

[Bl35]   H.F. Blichfeldt, *The minimum value of positive quadratic forms in six, seven and eight variables*, Math. Z. **39** (1935) 1–15. MR1545485

[Br00]   G. Brinkmann, Isomorphism rejection in structure generation programs, *Discrete mathematical chemistry, DIMACS Ser. Discrete Math. Theoret. Comput. Sci.* **51** (Amer. Math. Soc., 2000) 25–38. MR1762931

[ChRo99]   C.S. Chan and D.P. Robbins, *On the volume of the polytope of doubly stochastic matrices*, Experiment. Math. **8-3** (1999) 291–300. MR1724161 (2000k:15048)

[ChLo97]   T. Christof and A. Löbel, *PORTA: Polyhedron representation transformation algorithm (ver 1.3.1)*, 1997, `http://www.zib.de/Optimization/Software/Porta/`.

[ChRe96]   T. Christof and G. Reinelt, *Combinatorial optimization and small polytopes*, Top (Spanish Statistical and Operations Research Society) **4** (1996) 1–64. MR1404262 (97g:90107)

[Co93]   H. Cohen, *A course in computational algebraic number theory*, Graduate texts in mathematics, Springer–Verlag, 1993. MR1228206 (94i:11105)

[CoKu04]   H. Cohn and A. Kumar, *Optimality and uniqueness of the Leech lattice among lattices*, `http://www.arxiv.org/math.MG/0403263`.

[CoSl98]   J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, third edition, volume 290 of *Grundlehren der mathematischen Wissenschaften*, Springer–Verlag, 1998. MR1662447 (2000b:11077)

[CoSl88]   J.H. Conway and N.J.A. Sloane, *Low-dimensional lattices. III. Perfect forms*, Proc. Roy. Soc. London Ser. A **418-1854** (1988) 43–80. MR953277 (90a:11073)

[Co51]   H.S.M. Coxeter, *Extreme forms*, Canad. J. Math. **3** (1951) 391–441. MR0044580 (13:443c)

[DeDu03]   M. Deza and M. Dutour, *Cones of metrics, hemi-metrics and super-metrics*, Annals of the European Academy of Sciences (2003) 141–162.

[DFPS01]   A. Deza, K. Fukuda, D. Pasechnik, and M. Sato, *On the skeleton of the metric polytope*, Lecture Notes in Computer Science **2098** Springer-Verlag, Berlin (2001) 125–136. MR2043643 (2004m:90121)

[Fu95]   K. Fukuda, *cdd+ reference manual*, Institute for operations research, Swiss Federal Institute of Technology, Zurich, Switzerland, 1995, `http://www.ifor.math.ethz.ch/~fukuda/cdd_home/cdd.html`.

[Ga40]   C.F. Gauss, *Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen von Ludwig August Seeber*, J. Reine Angew. Math. **20** (1840) 312–320.

[GAP05]   The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4.6; 2005. `http://www.gap-system.org`.

[Ja92]   D.O. Jaquet-Chiffelle, *Description des voisines de E_7, D_7, D_8 et D_9*, Sém. Théor. Nombres Bordeaux **4-2** (1992) 273–377. MR1208866 (94e:11035)

[Ja93]   D.O. Jaquet, *Énumération complète des formes parfaites en dimension* 7, Ann. Inst. Fourier **43-1** (1993) 21–55. MR1209694 (94d:11048)

[KaSc03]   V. Kaibel and A. Schwartz, *On the complexity of polytope isomorphism problems*, Graphs Comb. **19-2** (2003) 215–230. MR1996205 (2004e:05125)

[Ke99]   A. Kerber, *Applied finite group actions*, second edition, Algorithms and Combinatorics, Springer-Verlag, 1999. MR1716962 (2000j:05129)

[KoZo72]   A.N. Korkine and E.I. Zolotarev, *Sur les formes quadratiques positives quaternaires*, Math. Ann. **5** (1872) 581–583. MR1509795

[KoZo73]   A.N. Korkine and E.I. Zolotarev, *Sur les formes quadratiques*, Math. Ann. **6** (1873) 366–389. MR1509828

[KoZo77]   A.N. Korkine and E.I. Zolotarev, *Sur les formes quadratiques positives*, Math. Ann. **11** (1877) 242–292. MR1509914

[La73]   J.L. Lagrange, *Démonstration d'un théorème d'arithmétique*, Nouv. Mém. Acad. Berlin (1770), in Oeuvres de Lagrange III, 189–201.

[La92]   M. Laïhem, *Construction algorithmique des réseaux parfaits*, Thèse, Bordeaux, 1992.

[La71]   J. Larmouth, *The enumeration of perfect forms*, in: A.O.L. Atkin and B.J. Birch, eds., Proceedings of the Science Research Council Atlas Symposium No. 2 held at Oxford, 1969 (Academic Press, London-New York, 1971) 237–239. MR0314733 (47:3285)

[Ma03]   J. Martinet, *Perfect lattices in Euclidean spaces*, Springer, 2003. MR1957723 (2003m:11099)

[Ma97]   A. Marzetta, *pd - C-implementation of the primal dual algorithm*, 1997, `http://www.cs.unb.ca/profs/bremner/pd/`.

[MKa05]   B.D. McKay, *The nauty program*, `http://cs.anu.edu.au/people/bdm/nauty/`.

[Mo44]   L.J. Mordell, *Observation on the minimum of a positive quadratic forms in eight variables*, J. London Math. Soc. **19** (1944) 3–6. MR0010708 (6:57e)

[Na96]   H. Napias, *Étude expérimentale et algorithmique des réseaux Euclidiens*, Thèse, Bordeaux, 1996.

[PlOpSc98] W. Plesken, J. Opgenorth, and T. Schulz, *CARAT—a package for mathematical crystallography*, J. Appl. Cryst. **31** (1998) 827–828.

[PlSo97] W. Plesken and B. Souvignier, *Computing isometries of lattices*, J. Symbolic Computation **24** (1997) 327–334. MR1484483 (98i:11047)

[Ri06]   C. Riener, *On extreme forms in dimension* 8, to appear in J. Théorie des Nombres de Bordeaux, `http://www.math.u-bordeaux.fr/~martinet/riener4.pdf`.

[Ry70]   S.S. Ryshkov, *The polyhedron μ(m) and certain extremal problems of the geometry of numbers*, Soviet Math. Dokl. **11** (1970) 1240–1244, translation from Dokl. Akad. Nauk SSSR **194** (1970) 514–517. MR0276873 (43:2613)

[RyBa79] S.S. Ryshkov, E.P. Baranovski, *Classical methods in the theory of lattice packings*, Russian Math. Surveys **34** (1979) 1–68, translation of Uspekhi Mat. Nauk **34** (1979) 3–63. MR548416 (81a:10045)

[Sch86]   A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, 1986. MR874114 (88m:90090)

[Sh05]   N.I. Shepherd-Barron, *Perfect forms and the moduli space of abelian varieties*, Invent. Math. **163-1** (2006) 25–45. MR2208417 (2007e:14070)

[So05]   C. Soulé, *Perfect forms and the Vandiver conjecture*, J. Reine Angew. Math. **517** (1999) 209–221. MR1728540 (2001d:11102)

[Swa85]   G. Swart, *Finding the convex hull facet by facet*, J. Algorithms **6** (1985) 17–48. MR780849 (87c:68074)

[Va99]   F. Vallentin, *SHVEC*, `http://www.math.uni-magdeburg.de/lattice_geometry/`.

[Ve80]   N.M. Vetchinkin, *Uniqueness of the classes of positive quadratic forms on which the values of Hermite constants are attained for 6 ≤ n ≤ 8*, Proc. Steklov Inst. Math. **152** (1980) 34–86. MR603814 (82f:10040)

[Vo08]   G. Voronoi, *Nouvelles applications des paramètres continues à la théorie des formes quadratiques 1: Sur quelques propriétés des formes quadratiques positives parfaites*, J. Reine Angew. Math **133** (1908) 97–178.

[Wa71]   G.L. Watson, *The number of minimum points of a positive quadratic form*, Dissertationes Math. Rozprawy Mat. **84** (1971) 1–43. MR0318061 (47:6610)

[Zi95]   G. Ziegler, *Lectures on polytopes*, Springer Verlag, 1995. MR1311028 (96a:52011)

[Zo99]   C. Zong, *Sphere packings*, Springer Verlag, 1999. MR1707318 (2000g:52020)

Institut Rudjer Bošković, Zagreb, Croatia
E-mail address: `Mathieu.Dutour@ens.fr`

Otto-von-Guericke-University, Magdeburg, Germany
E-mail address: `Achill.Schuermann@Mathematik.Uni-Magdeburg.de`

CWI, Amsterdam, The Netherlands
E-mail address: `f.vallentin@cwi.nl`