# Computing with Arithmetic Groups

Gabriele Nebe
Lehrstuhl D für Mathematatik, RWTH Aachen University
52056 Aachen
Germany
nebe@math.rwth-aachen.de

**ACM Reference format:**
Gabriele Nebe. 2017. Computing with Arithmetic Groups. In *Proceedings of ISSAC, TU Kaiserslautern, Germany, July 2017 (ISSAC 2017)*, 2 pages.
https://doi.org/10.1145/nnnnnnn.nnnnnnn

## 1 PAIRS OF DUAL CONES

Around 1900 Voronoï [10] formulated his fundamental algorithm to enumerate all similarity classes of perfect lattices in a given dimension. This algorithm has far reaching generalisations ([7], [6], [4]) used to compute generators and relators for arithmetic groups.

A quite general situation, where one may apply Voronoï's algorithm, is described in [7]:

Let $\sigma : V_1 \times V_2 \to \mathbb{R}$ be a non-degenerate bilinear mapping on a pair of isomorphic finite-dimensional real vector spaces $V_1$, $V_2$. Two open non-empty subsets $P_i \subseteq V_i$ form a pair of dual cones, if $\sigma$ is strictly positive on $P_1 \times P_2$ and for all $f \in V_1 \setminus P_1, y \in V_2 \setminus P_2$ there are $f' \in \overline{P}_1$, $y' \in \overline{P}_2$ such that $\sigma(f, y') \leq 0$, $\sigma(f', y) \leq 0$.

We now fix a discrete subset $D \subseteq \overline{P}_2 \setminus \{0\}$. For $f \in P_1$ we define

- The minimum of $f$ as $\min(f) := \min\{\sigma(f,d) \mid d \in D\}$,
- $S(f) := \{d \in D \mid \sigma(f,d) = \min(f)\}$,
- and the Voronoï domain $V(f) := \{\sum_{d \in S(f)} a_d d \mid a_d \geq 0\}$.
- The element $f$ is called *perfect*, if $S(f)$ spans $V_2$, so if $V(f)$ has a non-empty interior.
- $P_D := \{f \in P_1 \mid \min(f) = 1, f \text{ is perfect }\}$ denotes the set of perfect elements of minimum 1.

In his original application Voronoï aimed to classify all locally densest lattices. Here

$$P_1 = P_2 = \{f \in \mathbb{R}^{n \times n}_{\text{sym}} \mid f \text{ is positive definite }\}$$

is the cone of positive definite symmetric real matrices, $V_i = \mathbb{R}^{n \times n}_{\text{sym}}$,

$$\sigma : V_1 \times V_2 \to \mathbb{R}, \sigma(x,y) = \text{Tr}(xy)$$

is the trace bilinear form and the set $D$ is

$$D = \{x^{tr}x \mid 0 \neq x \in \mathbb{Z}^n\}.$$

Then for $f \in P_1$ and $x \in \mathbb{Z}^n$ we compute

$$\sigma(f, x^{tr}x) = \text{Tr}(f(x^{tr}x)) = \text{Tr}(xfx^{tr}) = xfx^{tr} = f[x]$$

the value of the quadratic form $f$ evaluated at the point $x$.


*ISSAC 2017, July 2017, TU Kaiserslautern, Germany*

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM.
https://doi.org/10.1145/nnnnnnn.nnnnnnn

An important point is the admissibility of $D$, where $D$ is called *admissible* if for any sequence $(f_i)_{i \in \mathbb{N}}$ of elements in $P_1$ converging to the boundary of $P_1$ the sequence $\min(f_i)$ converges to 0.

In this very general situation, the main result of Voronoï theory remains true:

Theorem 1.1. *([7, Theorem 1.9]) Let $D \subset \overline{P}_2 \setminus \{0\}$ be a discrete admissible set. Then the Voronoï domains of the perfect elements in $P_1$ form an exact tessellation of $P_2$.*

Exact means that every codimension 1 face of any $V(x)$ is contained in exactly one other $V(y)$ and it is again a face of $V(y)$. In this case $x, y \in P_D$ are called *neighbours*. The Voronoï graph $\Gamma_D$ has vertices $P_D$. Two vertices $x, y \in P_D$ are connected by an edge in $\Gamma_D$ if and only if they are neighbours. Then $\Gamma_D$ is a connected, locally finite graph.

## 2 DISCONTINUOUS GROUPS

Assume that we have a subgroup

$$\Omega \leq \text{Aut}(P_1) := \{g \in \text{GL}(V_1) \mid P_1 g = P_1\}$$

that acts properly discontinuously on $P_1$, i.e. the stabilizer in $\Omega$ of any point in $P_1$ is finite and the orbit $f\Omega$ ($f \in P_1$) has no cluster point. Choose $D \subset \overline{P}_2 \setminus \{0\}$ discrete, admissible and invariant under the adjoint group $\Omega^{ad} \leq \text{Aut}(P_2)$. Recall that for $g \in \text{Aut}(P_1)$ the element $g^{ad}$ is the unique element in $\text{Aut}(P_2)$ such that $\sigma(fg, y) = \sigma(f, yg^{ad})$ for all $f \in V_1, y \in V_2$. Then $\Omega$ acts on $P_D$. Assume that there are only finitely many orbits. Then we may choose representatives $R := \{f_1, \ldots, f_t\}$ of these $\Omega$ orbits on $P_D$ that form the vertices of a connected subtree of $\Gamma_D$. Let $T \subset P_D \setminus R$ be the (finite) set of all vertices in $\Gamma_D$ that are neighbours of some element of $R$. Then for each $f \in T$ there is some $\omega_f \in \Omega$ such that $f\omega_f \in R$ and

Theorem 2.1. *(see [7, Theorem 2.2])*

$$\Omega = \langle \text{Stab}_\Omega(f_i), \omega_f \mid 1 \leq i \leq t, f \in T \rangle.$$

To turn this theorem into a constructive algorithm one needs to be able to fulfill the following tasks

(a) Find some element $f \in P_D$.
(b) Compute the stabiliser in $\Omega$ of an element $f \in P_D$.
(c) Find all neighbors $y$ of $f$ (up to the action of $\text{Stab}_\Omega(f)$).
(d) Check for all $y$ whether there is some $\omega \in \Omega$ such that $y\omega$ is already known.

Problems (b) and (d) often can be solved by computing isometries of lattices in Euclidean spaces (see [8]).

Defining relations are obtained using Bass-Serre theory by walking around the codimension 2 faces of the Voronoï domains of the elements in $R$ (see [5]). For more details the reader is referred to [4], in particular [4, Theorem 4.1].

The infrastructure provided by the Voronoï algorithm can be used for a constructive membership test: Given some element $g \in \mathrm{Aut}(P_1)$ decide whether $g \in \Omega$ and express $g$ as a word in the generators from Theorem 2.1. This problem can be solved as follows:

(1) Put $\mathcal{F} := \bigcup_{i=1}^t \overline{V(f_i)}$.
(2) Choose some $p$ in the interior of $\mathcal{F}$.
(3) Compute $q := pg^{ad} \in P_2$.
(4) The geodesics $\mathcal{G} := \{p + s(p-q) \mid s \in [0,1]\} \subset P_2$ intersect the boundary of $\mathcal{F}$ in some point which is very likely in the relative interior of a codimension 1 face of some $V(f_i)$.
(5) Let $f \in T$ be the neighbour of $f_i$ corresponding to this face. Then $p\omega_f^{ad}$ is "closer" to $q$ than $p$.
(6) Replace $g$ by $\omega_f^{-1} g$ and repeat from Step (3).

For more details see [4, Section 5].

## 3 APPLICATIONS

### 3.1 The integral normaliser [7]

Let $G \leq \mathrm{GL}_n(\mathbb{Z})$ be some finite unimodular group and put

$$V_1 := \mathcal{F}(G) := \{F \in \mathbb{R}^{n\times n}_{\mathrm{sym}} \mid gFg^{tr} = F \text{ for all } g \in G\}$$

the space of $G$-invariant forms. Then

$$P_1 := \{F \in V_1 \mid F \text{ is positive definite }\}$$

is a non-empty open cone in $V_1$ spanning $V_1$ as a vector space. The Bravais group

$$B(G) = \{g \in \mathrm{GL}_n(\mathbb{Z}) \mid gFg^{tr} = F \text{ for all } F \in \mathcal{F}(G)\}$$

is hence a finite overgroup of $G$. The integral normaliser

$$N_{\mathrm{GL}_n(\mathbb{Z})}(G) := \{g \in \mathrm{GL}_n(\mathbb{Z}) \mid gGg^{-1} = G\}$$

acts on $\mathcal{F}(G)$ and $N_{\mathrm{GL}_n(\mathbb{Z})}(G)$ is a finite index subgroup of

$$\Omega := N_{\mathrm{GL}_n(\mathbb{Z})}(B(G)) = \{g \in \mathrm{GL}_n(\mathbb{Z}) \mid gP_1g^{tr} = P_1\} \leq \mathrm{Aut}(P_1).$$

To obtain a natural dual cone we take $V_2 := \mathcal{F}(G^{tr})$, $P_2$ the positive definite elements in $V_2$ and

$$\sigma : V_1 \times V_2 \to \mathbb{R}, (F_1, F_2) \mapsto \mathrm{Tr}(F_1F_2).$$

Then

$$D = \{\pi_x := \frac{1}{|G|} \sum_{g\in G} (xg)^{tr}(xg) \mid 0 \neq x \in \mathbb{Z}^n\}$$

is a discrete admissible subset of $\overline{P}_2 \setminus \{0\}$ (see [7, Section 3]) and $\sigma(F, \pi_x) = F[x]$ for all $x \in \mathbb{Z}^n$, $F \in V_1$.

### 3.2 Automorphism groups of hyperbolic lattices, see [6]

### 3.3 Cohomology of arithmetic groups

There are many contributions based on [2].

### 3.4 Unit groups of orders [4]

Let $K$ be a number field with ring of integers $\mathbb{Z}_K$, $\mathcal{A}$ be some simple $K$-algebra and $\Lambda \subseteq \mathcal{A}$ a $\mathbb{Z}_K$-order. The paper [4] uses the ideas from Section 2 to compute the unit group $\Omega = \Lambda^*$ of the ring $\Lambda$. The algebra $\mathcal{A}_{\mathbb{R}} := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R}$ is a semisimple $\mathbb{R}$-algebra, so it is isomorphic to a direct sum of matrix rings over $\mathbb{R}$, $\mathbb{C}$ or the Hamilton quaternion algebra $\mathbb{H}$. Any choice of such an isomorphism defines a "canonical" involution, $^\dagger$, on $\mathcal{A}_{\mathbb{R}}$, the transposition of the matrices composed by the identity, the complex conjugation or the quaternionic conjugation of the entries. Though in general $\mathcal{A}^\dagger \neq \mathcal{A}$, the unit group $\mathcal{A}^*$ and its subgroup $\Lambda^*$ act on the space of symmetric elements

$$V_1 = V_2 := \{F \in \mathcal{A}_{\mathbb{R}} \mid F^\dagger = F\}$$

by $(F, g) \mapsto g^\dagger F g$. This space supports the positive definite inner product

$$\sigma : V_1 \times V_2 \to \mathbb{R}, (F_1, F_2) \mapsto \mathrm{Tr}(F_1F_2)$$

where $\mathrm{Tr} = \mathrm{Tr}_{\mathcal{A}_{\mathbb{R}}/\mathbb{R}}$ is the reduced trace. Let $M$ be the simple $\mathcal{A}$-module. Then any $F \in V_i$ defines a quadratic form on $M_{\mathbb{R}}$ by $F[x] := \sigma(F, xx^\dagger)$ and the sets $P_i$ of elements in $V_i$ for which this quadratic form is positive definite forms a pair of dual cones.

For any $\Lambda$-lattice $L \leq M$ the set

$$D := \{xx^\dagger \mid 0 \neq x \in L\}$$

is an admissible discrete $\Omega^{ad} = (\Lambda^\dagger)^*$-invariant set $D \subset \overline{P_2} \setminus \{0\}$.

### 3.5 $S$-arithmetic groups

In the situation of 3.4 let $S = \{\wp_1, \ldots, \wp_s\}$ be some finite set of finite places of the number field $K$ and put

$$\mathbb{Z}_{K,S} := \{a \in K \mid ||a||_\wp \leq 1 \text{ for all } \wp \notin S\}$$

the ring of $S$-integers in $K$.

Then the $S$-unit group of $\Lambda$ is the group of invertible elements in $\Lambda_S := \mathbb{Z}_{K,S} \otimes_{\mathbb{Z}_K} \Lambda$. This is an example of an $S$-arithmetic group.

In the 1970s Borel and Serre [3] used actions of $S$-arithmetic groups on certain contractible CW-complexes to prove finiteness results for these groups. In our special situation this CW-complex is constructed in the product $\mathcal{X} \times \prod_{i=1}^s \mathcal{X}_i$, where the factor $\mathcal{X}$ could be replaced by the rational closure of the cone $P_2$ from 3.4 and the $\mathcal{X}_i$ are the Bruhat-Tits buildings of the groups $\mathrm{SL}(\mathcal{A}_{\wp_i})$. In particular these $\mathcal{X}_i$ are simplicial complexes and one can use the lattice chain model from [1] to explicitly compute in these buildings. In combination with the algorithm in [4] this allows us to make the results from Borel and Serre constructive and compute presentations also for $\Lambda_S^*$. The design and implementation of the corresponding algorithms is work in progress [9].

## REFERENCES

[1] P. Abramenko, G. Nebe, *Lattice chain models for affine buildings of classical type.* Math. Ann. 322 (2002) 537–562.
[2] A. Ash, *Small-dimensional classifying spaces for arithmetic subgroups of general linear groups.* Duke Math. J. 51 (1984) 459–468.
[3] A. Borel, J.-P. Serre, *Cohomologie d'immeubles et de groupes S-arithmétiques.* Topology 15 (1976) 211–232.
[4] O. Braun, R. Coulangeon, G. Nebe, S. Schönnenbeck. *Computing in arithmetic groups with Voronoï's algorithm.* J. Algebra 435 (2015) 263–285.
[5] K. S. Brown, *Presentations for groups acting on simply-connected complexes.* J. Pure Appl. Algebra 32 (1984) 1–10.
[6] M. Mertens, *Automorphism groups of hyperbolic lattices.* J. Algebra 408 (2014) 147–165.
[7] J. Opgenorth, *Dual cones and the Voronoi algorithm.* Experiment. Math. 10 (2001) 599–608.
[8] W. Plesken, B. Souvignier. *Computing isometries of lattices.* Computational algebra and number theory (London, 1993). J. Symbolic Comput. 24 (1997) 327–334.
[9] S. Schönnenbeck, *Computing S-unit groups of orders.* (in preparation)
[10] G. F. Voronoï, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques : 1 sur quelques propriétés des formes quadratiques parfaites*, J. Reine Angew. Math. 133 (1907) 97–178.