Voronoi's algorithm to compute perfect lattices

- $F \in \mathbb{R}^{n\times n}_{sym,>0}$
- $\min(F) := \min\{xFx^{tr} \mid 0 \neq x \in \mathbb{Z}^n\}$ minimum
- $\mathrm{Min}(F) := \{x \in \mathbb{Z}^n \mid xFx^{tr} = \min(F)\}$.
- $\mathrm{Vor}(F) :=$ conv $(x^{tr}x \mid x \in \mathrm{Min}(F))$ Voronoi domain
- F perfect, if and only if $\dim(\mathrm{Vor}(F)) = n(n+1)/2$.
- $\mathcal{P}_n := \{F \in \mathbb{R}^{n\times n}_{sym,>0} \mid \min(F) = 1, F$ perfect $\}$.

Theorem (Voronoi)

$\underline{\mathcal{T}_n := \{}\mathrm{Vor}(F) \mid F \in \mathcal{P}_n\}$ is a locally finite, face to face tessellation of $\mathbb{R}^{n\times n}_{sym,>0}$ on which $\mathrm{GL}_n(\mathbb{Z})$ acts with finitely many orbits.

- $\mathrm{Min}(gFg^{tr}) = \{xg^{-1} \mid x \in \mathrm{Min}(F)\}$ so
- $\mathrm{Vor}(gFg^{tr}) = g^{-tr}\,\mathrm{Vor}(F)g^{-1}$

Max Koecher: Pair of dual cones

Jürgen Opgenorth: “Dual cones and the Voronoi Algorithm”
Experimental Mathematics 2001

- $\mathcal{V}_1, \mathcal{V}_2$ real vector spaces of same dimension n
- $\sigma : \mathcal{V}_1 \times \mathcal{V}_2 \longrightarrow \mathbb{R}$ bilinear and non-degenerate.

Definition

$\mathcal{V}_1^{>0} \subset \mathcal{V}_1$ and $\mathcal{V}_2^{>0} \subset \mathcal{V}_2$ are dual cones if

(DC1) $\mathcal{V}_i^{>0}$ is open in $\mathcal{V}_i$ and non-empty for i=1,2.

(DC2) For all $x \in \mathcal{V}_1^{>0}$ and $y \in \mathcal{V}_2^{>0}$ one has $\sigma(x, y) > 0$.

(DC3) For every $x \in \mathcal{V}_1 - \mathcal{V}_1^{>0}$ there is $0 \neq y \in \mathcal{V}_2^{>0}$ with $\sigma(x, y) \leq 0$
for every $y \in \mathcal{V}_2 - \mathcal{V}_2^{>0}$ there is $0 \neq x \in \mathcal{V}_1^{>0}$ with $\sigma(x, y) \leq 0$.

$\mathcal{V}_1^{>0}$ and $\mathcal{V}_2^{>0}$ pair of dual cones

Let $D \subset \mathcal{V}_2^{\geq 0} - \{0\}$ be discrete in $\mathcal{V}_2$ and $x \in \mathcal{V}_1^{>0}$.

- $\mu_D(x) := \min\{\sigma(x,d) \mid d \in D\}$ the D-minimum of x.
- $M_D(x) := \{d \in D \mid \mu_D(x) = \sigma(x,d)\}$
  the set of D-minimal vectors of x.
- $M_D(x)$ is finite and $M_D(x) = M_D(\lambda x)$ for all $\lambda > 0$.
- $V_D(x) := \{\sum_d a_d d \mid d \in M_D(x), a_d \in \mathbb{R}^{>0}\}$
  the D-Voronoi domain of x.
- A vector $x \in \mathcal{V}_1^{>0}$ is called D-perfect, if codim$(V_D(x)) = 0$.

$$P_D := \{x \in \mathcal{V}_1^{>0} \mid \mu_D(x) = 1, x \text{ is D-perfect } \}$$

Definition

D is called admissible if for every sequence $(x_i)_{i \in \mathbb{N}}$ that converges to a point $x \in \delta\mathcal{V}_1^{>0}$ the sequence $(\mu_D(x_i))_{i \in \mathbb{N}}$ converges to 0.

Voronoi tessellation

Theorem

If $D \subset \mathcal{V}_2^{\geq 0} - \{0\}$ is discrete in $\mathcal{V}_2$ and admissible then the D-Voronoi domains of the D-perfect vectors form an exact tessellation of $\mathcal{V}_2^{\geq 0}$.

Definition

The graph Γ_D of D-perfect vectors has vertices P_D and edges

$$E = \{(x, y) \in P_D \times P_D \mid x \text{ and } y \text{ are neighbours } \}.$$

Here $x, y \in P_D$ are neighbours if codim($V_D(x) \cap V_D(y)$) = 1.

Corollary

If $D \subseteq \mathcal{V}_2^{\geq 0} - \{0\}$ is discrete and admissible then Γ_D is a connected, locally finite graph.

Discontinuous Groups

- $\mathrm{Aut}(\mathcal{V}_i^{>0}) := \{g \in \mathrm{GL}(\mathcal{V}_i) \mid \mathcal{V}_i^{>0} g = \mathcal{V}_i^{>0}\}$.
- $\Omega \leq \mathrm{Aut}(\mathcal{V}_1^{>0})$ properly discontinously on $\mathcal{V}_1^{>0}$.
- $\Omega^{ad} := \{\omega^{ad} \mid \omega \in \Omega\} \leq \mathrm{Aut}(\mathcal{V}_2^{>0}$
- $D \subseteq \mathcal{V}_2^{\geq 0} - \{0\}$ discrete, admissible and invariant under Ω^{ad}
- For $x \in \mathcal{V}_1^{>0}$ and $\omega \in \Omega$ we have
- $\mu_D(xw) = \mu_D(x)$,
- $M_D(xw) = M_D(x)(\omega^{ad})^{-1}$,
- $V_D(xw) = V_D(x)(\omega^{ad})^{-1}$.
- In particular Ω acts on Γ_D.

Discontinuous Groups (continued)

Theorem

- Assume additionally that the residue graph Γ_D/Ω is finite.
- $x_1, \ldots, x_t \in P_D$ orbit representatives spanning a connected subtree T of Γ_D
- $\delta T := \{y \in P_D - T \mid y$ neighbour of some $x_i \in T\}$.
- $\omega_y \in \Omega$ with $y\omega_y \in T$.
- $\Omega = \langle \omega_y, \mathrm{Stab}_\Omega(x) \mid x \in T, y \in \delta T \rangle$
- In particular the group Ω is finitely generated.

Applications

Jürgen Opgenorth, 2001

$G \leq \mathrm{GL}_n(\mathbb{Z})$ finite. Compute $\Omega := N_{\mathrm{GL}_n(\mathbb{Z})}(G)$.

Michael Mertens, 2014

$L \leq (\mathbb{R}^{n+1}, \sum_{i=1}^{n} x_i^2 - x_{n+1}^2) =: H^{n+1}$ a $\mathbb{Z}$-lattice in hyperbolic space (signature $(n, 1)$).
Compute $\Omega := \mathrm{Aut}(L) := \{g \in O(H^{n+1}) \mid Lg = L\}$.

Braun, Coulangeon, N., Schönnenbeck, 2015

A finite dimensional semisimple $\mathbb{Q}$-algebra, $\Lambda \leq A$ order, i.e. a finitely generated full $\mathbb{Z}$-lattice that is a subring of A. Compute
$\Omega := \Lambda^* := \{g \in \Lambda \mid \exists h \in \Lambda, gh = hg = 1\}$.

Normalizers of finite unimodular groups

- $G \leq \mathrm{GL}_n(\mathbb{Z})$ finite.
- $\mathcal{F}(G) := \{F \in \mathbb{R}^{n\times n}_{sym} \mid gFg^{tr} = F \text{ for all } g \in G\}$
  space of invariant forms.
- $\mathcal{B}(G) := \{g \in \mathrm{GL}_n(\mathbb{Z}) \mid gFg^{tr} = F \text{ for all } F \in \mathcal{F}(G)\}$
  Bravais group.
- $\mathcal{F}(G)$ always contains a positive definite form $\sum_{g\in G} gg^{tr}$.
- $\mathcal{B}(G)$ is finite.
- $N_{\mathrm{GL}_n(\mathbb{Z})}(G) \leq N_{\mathrm{GL}_n(Z)}(\mathcal{B}(G)) =: \Omega$ acts on $\mathcal{F}(G)$.
- Compute Ω and then the finite index subgroup $N_{\mathrm{GL}_n(\mathbb{Z})}(G)$.
- $\mathcal{V}_1 := \mathcal{F}(G)$ and $\mathcal{V}_2 := \mathcal{F}(G^{tr})$.
- $\sigma : \mathcal{V}_1 \times \mathcal{V}_2 \to \mathbb{R}_{>0}, \sigma(A, B) := \mathrm{trace}(AB)$.
- $\pi : \mathbb{R}^{n\times n}_{sym} \to \mathcal{V}_2,\ F \mapsto \frac{1}{|G|} g^{tr} F g$
- $A \in \mathcal{F}(G), B \in \mathbb{R}^{n\times n}_{sym} \Rightarrow \sigma(A, \pi(B)) = \mathrm{trace}(AB)$
- $D := \{q_x := \pi(x^{tr}x) \mid x \in \mathbb{Z}^{1\times n}\}$
- $F \in \mathcal{F}(G) \cap \mathbb{R}^{n\times n}_{sym,>0}$ then $\mu_D(F) = \min(F)$.

Easy example

- $G = \langle \mathrm{diag}(1,-1) \rangle$
- $\mathcal{F}(G) = \langle \mathrm{diag}(1,1), \mathrm{diag}(0,1) \rangle$
- $\mathcal{B}(G) = \langle \mathrm{diag}(1,-1), \mathrm{diag}(-1,-1) \rangle$
- $F = I_2$ is G-perfect.
- $V_D(F) = \mathcal{F}_{>0}(G^{tr})$.
- $N_{\mathrm{GL}_2(\mathbb{Z})}(G) \leq \Omega = N_{\mathrm{GL}_2(\mathbb{Z})}(\mathcal{B}(G)) = \mathrm{Aut}(F) \cong D_8$.

Orders in semi-simple rational algebras.

The positive cone

- K some rational division algebra, $A = K^{n\times n}$
- $A_{\mathbb{R}} := A \otimes_{\mathbb{Q}} \mathbb{R}$ semi-simple real algebra
- $A_{\mathbb{R}} \cong$ direct sum of matrix rings over of $\mathbb{H}$, $\mathbb{R}$ or $\mathbb{C}$.
- $A_{\mathbb{R}}$ carries a "canonical" involution † depending on the choice of the isomorphism that we use to define symmetric elements:
- $\mathcal{V}_1 = \mathcal{V}_2 = \mathcal{V} := \mathrm{Sym}(A_{\mathbb{R}}) := \left\{F \in A_{\mathbb{R}} \mid F^\dagger = F\right\}$
- $\sigma(F_1, F_2) := \mathrm{trace}(F_1 F_2)$ defines a Euclidean inner product on $\mathcal{V}$.
- In general the involution † will not fix the set A.

Orders: Endomorphism rings of lattices.

The simple A-module.

- Let $V = K^{1\times n}$ denote the simple right A-module, $V_{\mathbb{R}} = V \otimes_{\mathbb{Q}} \mathbb{R}$.
- For $x \in V$ we have $x^{\dagger}x \in \mathcal{V}$.
- $F \in \mathcal{V}$ is called positive if

$$F[x] := \sigma(F, x^{\dagger}x) > 0 \text{ for all } 0 \neq x \in V_{\mathbb{R}}.$$

- $\mathcal{V}^{>0} := \{F \in \mathcal{V} \mid F \text{ is positive } \}$.

The discrete admissible set

- $\mathcal{O}$ order in K, L some $\mathcal{O}$-lattice in the simple A-module V
- $\Lambda := \mathrm{End}_{\mathcal{O}}(L)$ is an order in A with unit group
  $\Lambda^* := \mathrm{GL}(L) = \{a \in A \mid aL = L\}$.

Minimal vectors.

L-minimal vectors

Let $F \in \mathcal{V}^{>0}$.

- $\mu(F) := \mu_L(F) = \min\{F[\ell] \mid 0 \neq \ell \in L\}$ the L-minimum of F
- $\mathcal{M}_L(F) := \{\ell \in L \mid F[\ell] = \mu_L(F)\}$ L-minimal vectors
- $\mathrm{Vor}_L(F) := \{\sum_{x \in \mathcal{M}_L(F)} a_x x^\dagger x \mid a_x \geq 0\} \subset \mathcal{V}^{\geq 0}$ Voronoi domain
- F is called L-perfect $\Leftrightarrow \dim(\mathrm{Vor}_L(F)) = \dim(\mathcal{V})$.

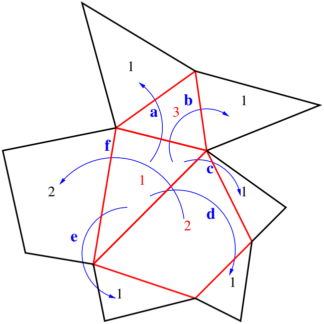
Theorem

$$\mathcal{T} := \{\mathrm{Vor}_L(F) \mid F \in \mathcal{V}^{>0},\ \text{L-perfect}\ \}$$

forms a locally finite face to face tessellation of $\mathcal{V}^{\geq 0}$.
Λ^* acts on $\mathcal{T}$ with finitely many orbits.

Generators for Λ^*

- Compute $\mathcal{R} := \{F_1, \dots, F_s\}$ set of representatives of Λ^*-orbits on the L-perfect forms, such that their Voronoi-graph is connected.
- For all neighbors F of one of these F_i (so $\mathrm{Vor}(F) \cap \mathrm{Vor}(F_i)$ has codimension 1) compute some $g_F \in \Lambda^*$ such that $g_F \cdot F \in \mathcal{R}$.
- Then $\Lambda^* = \langle \mathrm{Aut}(F_i), g_F \mid F_i \in \mathcal{R}, F \text{ neighbor of some } F_j \in \mathcal{R} \rangle$.



so here $\Lambda^* = \langle \mathrm{Aut}(F_1), \mathrm{Aut}(F_2), \mathrm{Aut}(F_3), a, b, c, d, e, f \rangle$.

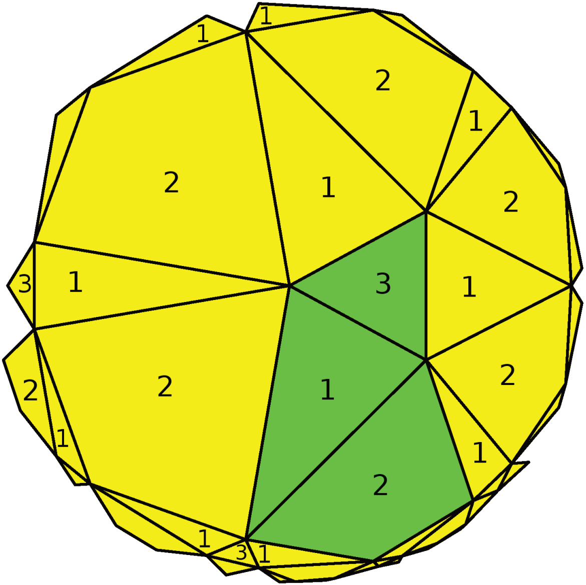
Example $\mathcal{Q}_{2,3}$.

- Take the rational quaternion algebra ramified at 2 and 3,

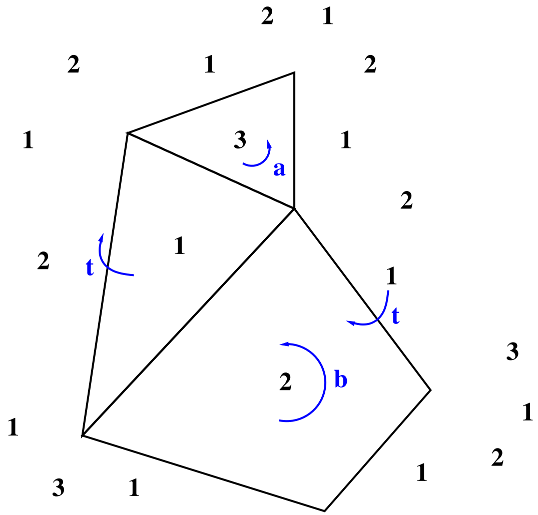
  $$\mathcal{Q}_{2,3} = \langle i, j \mid i^2 = 2, j^2 = 3, ij = -ji \rangle = \langle \mathrm{diag}(\sqrt{2}, -\sqrt{2}), \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \rangle$$

  Maximal order $\Lambda = \langle 1, i, \frac{1}{2}(1+i+ij), \frac{1}{2}(j+ij) \rangle$
- $V = A = \mathcal{Q}_{2,3}$, $A_{\mathbb{R}} = \mathbb{R}^{2\times 2}$, $L = \Lambda$
- Embed A into $A_{\mathbb{R}}$ using the maximal subfield $\mathbb{Q}[\sqrt{2}]$.
- Get three perfect forms:
- $F_1 = \begin{pmatrix} 1 & 2-\sqrt{2} \\ 2-\sqrt{2} & 1 \end{pmatrix}, F_2 = \begin{pmatrix} 6-3\sqrt{2} & 2 \\ 2 & 2+\sqrt{2} \end{pmatrix}$
- $F_3 = \mathrm{diag}(-3\sqrt{2}+9, 3\sqrt{2}+5)$

The tesselation for $\mathcal{Q}_{2,3} \hookrightarrow \mathbb{Q}[\sqrt{2}]^{2\times 2}$.



$$\Lambda^*/\langle \pm 1 \rangle = \langle a, b, t \mid a^3, b^2, atbt \rangle$$



$\Lambda^* = \langle a, b, t \mid a^3 = b^2 = atbt = -1 \rangle$, $A \cong \mathfrak{Q}_{2,3}$

$$a = \frac{1}{2} \begin{pmatrix} 1 & \sqrt{2}+1 \\ 3-3\sqrt{2} & 1 \end{pmatrix}$$

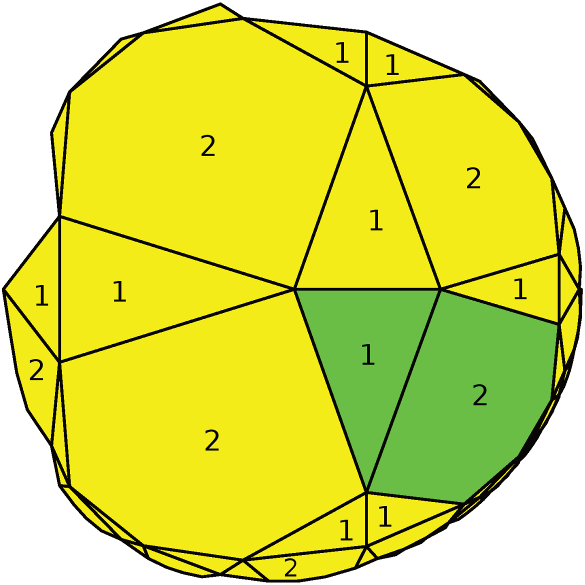
$$b = \begin{pmatrix} \sqrt{2} & \sqrt{2}+1 \\ 3-3\sqrt{2} & -\sqrt{2} \end{pmatrix}$$

$$t = \frac{1}{2} \begin{pmatrix} 2\sqrt{2}+1 & \sqrt{2}+1 \\ 3-3\sqrt{2} & 1-2\sqrt{2} \end{pmatrix}$$

Note that $t = b - a + 1$ has minimal polynomial $x^2 + x - 1$ and

$$\langle a, b \rangle / \langle \pm 1 \rangle \cong C_3 * C_2 \cong \mathrm{PSL}_2(\mathbb{Z})$$

The tesselation for $\mathcal{Q}_{2,3} \hookrightarrow \mathbb{Q}[\sqrt{3}]^{2\times 2}$.



A rational division algebra of degree 3

- $\vartheta = \zeta_9 + \zeta_9^{-1}$, $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{Q}(\vartheta)/\mathbb{Q})$,
- $\mathcal{A}$ the $\mathbb{Q}$-algebra generated by
- $Z := \begin{pmatrix} \vartheta & & \\ & \sigma(\vartheta) & \\ & & \sigma^2(\vartheta) \end{pmatrix}$ and $\Pi := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$.
- $\mathcal{A}$ division algebra, Hasse-invariants $\frac{1}{3}$ at 2 and $\frac{2}{3}$ at 3.
- Λ some maximal order in $\mathcal{A}$
- $\Gamma := \Lambda^\times$ has 431 orbits of perfect forms and presentation
- $$\begin{aligned}\Gamma \cong \langle a, b \mid\ & b^2a^2(b^{-1}a^{-1})^2,\ b^{-2}(a^{-1}b^{-1})^2ab^{-2}a^2b^{-3}, \\ & ab^2a^{-1}b^3a^{-2}bab^3,\ a^2bab^{-2}ab^{-1}(a^{-2}b)^2, \\ & a^{-1}b^2a^{-1}b^{-1}a^{-5}b^{-2}a^{-3}, \\ & b^{-2}a^{-2}b^{-1}a^{-1}b^{-1}a^{-2}b^{-1}a^{-1}b^{-2}(a^{-1}b^{-1})^3\rangle\end{aligned}$$
- $a = \frac{1}{3}((1-3Z-Z^2)+(2+Z^2)\Pi+(1-Z^2)\Pi^2)$,
  $b = \frac{1}{3}((-3-2Z+Z^2)+(1-2Z)\Pi+(1-Z^2)\Pi^2)$.

Quaternion algebras over CM fields

K CM-field and $\mathcal{A} = \mathcal{Q} \otimes K$ where $\mathcal{Q}$ is a definite quaternion algebra over the rationals.

$$\dagger : \mathcal{Q} \otimes K \to \mathcal{Q} \otimes K ; a \otimes k \mapsto \overline{a} \otimes \overline{k}$$

is a positive involution on $\mathcal{A}$.

$K = \mathbb{Q}\sqrt{-7}]$

- $\mathcal{A} = \left(\frac{-1,-1}{\mathbb{Q}[\sqrt{-7}]}\right) = \langle 1, i, j, k \rangle$, Λ maximal order
- only one orbit of perfect forms
- $\Lambda^{\times} = \langle a, b \mid b^3 = -1, (b^{-1}a^{-1}ba)^2 = -1, (b^2a^{-2})^3 = -1 \rangle$
- $a := \frac{1}{4}((1 + \sqrt{-7}) - (1 + \sqrt{-7})i + (1 + \sqrt{-7})j + (3 - \sqrt{-7})k)$,
- $b := \frac{1}{2}(1 + i - 3j + \sqrt{-7}k)$

Quaternion algebras over imaginary quadratic fields

$$\mathcal{A} = \left(\frac{-1,-1}{k}\right), \quad k = \mathbb{Q}(\sqrt{-d})$$

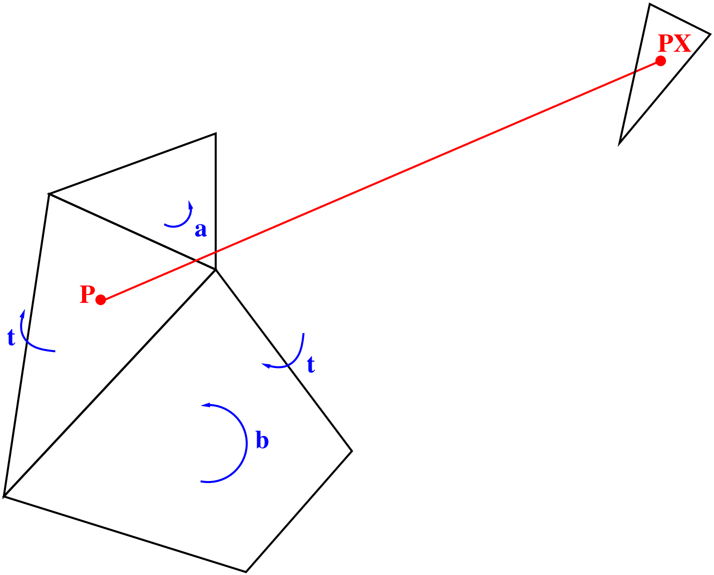
d	Number of perfect forms	Runtime Voronoï	Runtime Presentation	Number of generators
7	1	$1.24s$	$0.42s$	2
31	8	$6.16s$	$0.50s$	3
55	21	$14.69s$	$1.01s$	5
79	40	$28.74s$	$1.78s$	5
95	69	$53.78s$	$2.57s$	7
103	53	$38.39s$	$2.52s$	6
111	83	$66.16s$	$3.02s$	6
255	302	$323.93s$	$17.54s$	16

Quaternion algebras over $\mathbb{Q}(\sqrt{-7})$

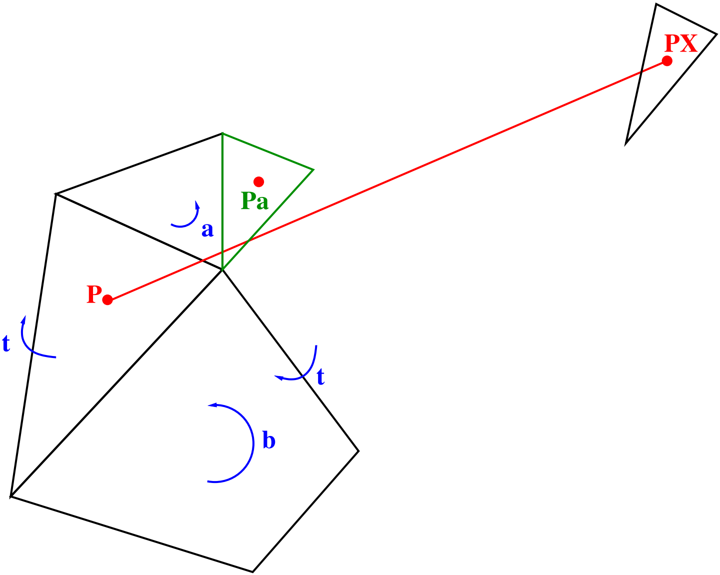
$$\mathcal{A} = \left(\frac{a, b}{\mathbb{Q}(\sqrt{-7})}\right)$$

a,b	perfect forms	Runtime Voronoï	Runtime Presentation	Number of generators
$-1, -1$	1	$1.24s$	$0.42s$	2
$-1, -11$	20	$21.61s$	$4.13s$	6
$-11, -14$	58	$51.46s$	$5.11s$	10
$-1, -23$	184	$179.23s$	$89.34s$	16

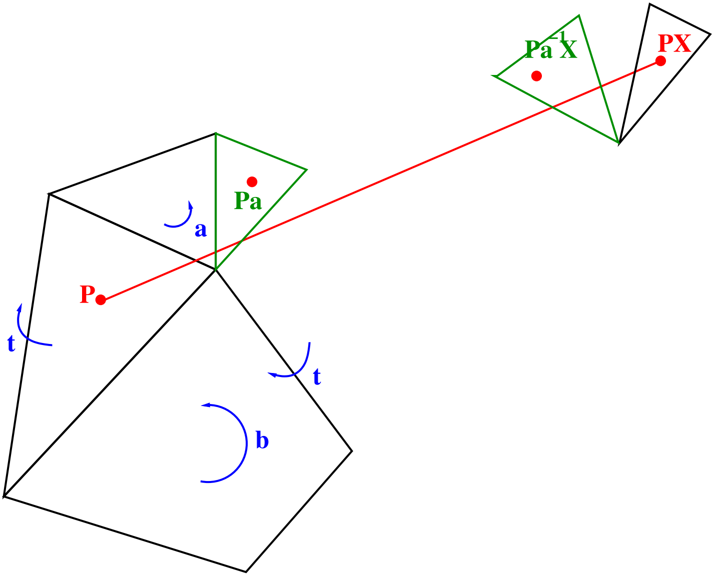
Easy solution of constructive recognition



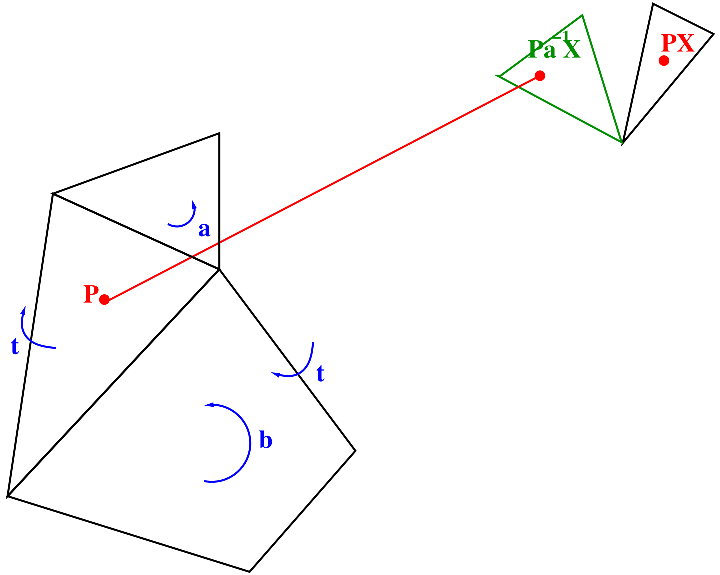
Easy solution of constructive recognition



Easy solution of constructive recognition



Easy solution of constructive recognition



Isomorphic unit groups

Question

Given two maximal orders Λ and Γ in $\mathcal{A}$. Does it hold that Λ^* is isomorphic to Γ^* if and only if Λ and Γ are conjugate in $\mathcal{A}$?

Maximal finite subgroups

$\Lambda^* \cong \Gamma^* \Rightarrow$ they have the same number of conjugacy classes of maximal finite subgroups G of given isomorphism type.
These G arise as stabilisers of well rounded faces of the Voronoi tessellation hence may be obtained by the Voronoi algorithm.

Integral Homology

Many people have used the Λ^* action on the subcomplex of well rounded faces of the Voronoi tessellation to compute $H_n(\Lambda^*, \mathbb{Z})$, which is again an invariant of the isomorphism class of Λ^*.

Conclusion

- Algorithm works quite well for indefinite quaternion algebras over the rationals
- Obtain presentation and algorithm to solve the word problem
- For $\mathcal{Q}_{19,37}$ our algorithm computes the presentation within 5 minutes (288 perfect forms, 88 generators) whereas the MAGMA implementation “FuchsianGroup” does not return a result after four hours
- Reasonably fast for quaternion algebras with imaginary quadratic center or matrix rings of degree 2 over imaginary quadratic fields
- For the rational division algebra of degree 3 ramified at 2 and 3 compute presentation of Λ^*, 431 perfect forms, 2 generators in about 10 minutes.
- Quaternion algebra with center $\mathbb{Q}[\zeta_5]$: > 40.000 perfect forms.
- Database available under `http://www.math.rwth-aachen.de/~Oliver.Braun/unitgroups/`
- Which questions can one answer for unit groups of orders?