Computing unit groups of orders

Gabriele Nebe

Lehrstuhl D für Mathematik

Bad Boll, 05.03.2014
The classical Voronoi Algorithm

- Around 1900 Korkine, Zolotareff, and Voronoi developed a reduction theory for quadratic forms.
- The aim was to classify the densest lattice sphere packings in \(n\)-dimensional Euclidean space.
- Lattice \(L = \mathbb{Z}^{1 \times n}\), Euclidean structure on \(L\) given by some positive definite \(F \in \mathbb{R}^{n \times n}_{\text{sym}}\), \((x, y) = xFy^t\).
- Voronoi described an algorithm to find all local maxima of the density function on the space of all \(n\)-dimensional positive definite \(F\).
- They are perfect forms (as will be defined below).
- There are only finitely many perfect forms up to the action of \(GL_n(\mathbb{Z})\), the unit group of the order \(\mathbb{Z}^{n \times n}\).
- Later, Voronoi’s algorithm has been used to compute generators and relations for \(GL_n(\mathbb{Z})\) but also its integral homology groups.
- It has been generalised to other situations: compute integral normalizer, the automorphism group of hyperbolic lattices and
- more general unit groups of orders.
Unit groups of orders

- A separable \( \mathbb{Q} \)-algebra, so \( A \cong \bigoplus_{i=1}^{s} D_{n_i}^{n_i} \), is a direct sum of matrix rings over division algebras.
- An order \( \Lambda \) in \( A \) is a subring that is finitely generated as a \( \mathbb{Z} \)-module and such that \( \langle \Lambda \rangle_{\mathbb{Q}} = A \).
- Its unit group is \( \Lambda^* := \{ u \in \Lambda \mid \exists v \in \Lambda, uv = 1 \} \).
- Know in general: \( \Lambda^* \) is finitely generated.
- Example: \( A = K \) a number field, \( \Lambda = O_K \), its ring of integers. Then Dirichlet’s unit theorem says that \( \Lambda^* \cong \mu_K \times \mathbb{Z}^{r+s-1} \).
- Example: \( \Lambda = \langle 1, i, j, ij \rangle_{\mathbb{Z}} \) with \( i^2 = j^2 = (ij)^2 = -1 \). Then \( \Lambda^* = \langle i, j \rangle \) the quaternion group of order 8.
- Example: \( A = \mathbb{Q}G \) for some finite group \( G \), \( \Lambda = \mathbb{Z}G \).
- Example: \( A \) a division algebra with \( \operatorname{dim}_{\mathbb{Z}(A)}(A) = d^2 > 4 \). Not much known about the structure of \( \Lambda^* \).
- Voronoi’s algorithm may be used to compute generators and relations for \( \Lambda^* \) and to solve the word problem.
- Seems to be practical for “small” \( A \) and for \( d = 3 \).
The classical Voronoi Algorithm
Korkine, Zolotareff, Voronoi, ~ 1900.

**Definition**

- $\mathcal{V} := \{ X \in \mathbb{R}^{n \times n} \mid X = X^{tr} \}$ space of symmetric matrices
- $\sigma : \mathcal{V} \times \mathcal{V} \to \mathbb{R}, \sigma(A, B) := \text{trace}(AB)$ Euclidean inner product on $\mathcal{V}$.
- for $F \in \mathcal{V}$, $x \in \mathbb{R}^{1 \times n}$ define $F[x] := xF x^{tr} = \sigma(F, x^{tr} x)$
- $\mathcal{V}^{>0} := \{ F \in \mathcal{V} \mid F \text{ positive definite } \}$
- for $F \in \mathcal{V}^{>0}$ define the minimum $\mu(F) := \min \{ F[x] : 0 \neq x \in \mathbb{Z}^{1 \times n} \}$ and $\mathcal{M}(F) := \{ x \in \mathbb{Z}^{1 \times n} \mid F[x] = \mu(F) \}$
- $\text{Vor}(F) := \{ \sum_{x \in \mathcal{M}(F)} a_x x^{tr} x \mid a_x \geq 0 \}$ the Voronoi domain
- $F$ is called perfect $\iff \dim(\text{Vor}(F)) = \dim(\mathcal{V}) = \frac{n(n+1)}{2}$.

**Remark**

$GL_n(\mathbb{Z})$ acts on $\mathcal{V}^{>0}$ by $(F, g) \mapsto g^{-1} F g^{-tr}$. Then

$\mathcal{M}(g^{-1} F g^{-tr}) = \{ xg \mid x \in \mathcal{M}(F) \}$

$\text{Vor}(g^{-1} F g^{-tr}) = g^{tr} \text{Vor}(F) g$
The classical Voronoi Algorithm
Korkine, Zolotareff, Voronoi, ~ 1900.

Definition

- $\mathcal{V} := \{X \in \mathbb{R}^{n \times n} | X = X^{tr}\}$ space of symmetric matrices
- $\sigma : \mathcal{V} \times \mathcal{V} \to \mathbb{R}$, $\sigma(A, B) := \text{trace}(AB)$ Euclidean inner product on $\mathcal{V}$.
- for $F \in \mathcal{V}$, $x \in \mathbb{R}^{1 \times n}$ define $F[x] := xf^{tr} = \sigma(F, x^{tr}x)$
- $\mathcal{V}^> := \{F \in \mathcal{V} | F$ positive definite $\}$
- for $F \in \mathcal{V}^>$ define the minimum $\mu(F) := \min\{F[x] : 0 \neq x \in \mathbb{Z}^{1 \times n}\}$ and $\mathcal{M}(F) := \{x \in \mathbb{Z}^{1 \times n} | F[x] = \mu(F)\}$
- $\text{Vor}(F) := \{\sum_{x \in \mathcal{M}(F)} a_xx^{tr}x | a_x \geq 0\}$ the Voronoi domain
- $F$ is called perfect $\iff \dim(\text{Vor}(F)) = \dim(\mathcal{V}) = \frac{n(n+1)}{2}$.

Theorem (Voronoi)

(a) $\mathcal{T} := \{\text{Vor}(F) | F \in \mathcal{V}^>, \text{perfect}\}$ forms a face to face tessellation of $\mathcal{V}^>$. 
(b) $\text{GL}_n(\mathbb{Z})$ acts on $\mathcal{T}$ with finitely many orbits that may be computed algorithmically.
Example, generators for $\text{GL}_2(\mathbb{Z})$

- $n = 2$, $\dim(V) = 3$, $\dim(V^{>0}/\mathbb{R}^{>0}) = 2$
- compute in affine section of the projective space
- $A^{\geq 0} = \{ F \in V^{\geq 0} | \text{trace}(F) = 1 \}$
- $F_0 = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$, $\mu(F_0) = 2$, $\mathcal{M}(F_0) = \{ \pm(1, 0), \pm(0, 1), \pm(1, 1) \}$
- $A^{\geq 0} \cap \text{Vor}(F_0) = \text{conv}(a = \begin{pmatrix} 10 \\ 00 \end{pmatrix}, b = \begin{pmatrix} 00 \\ 01 \end{pmatrix}, c = \frac{1}{2} \begin{pmatrix} 11 \\ 11 \end{pmatrix})$
Example, generators for $\text{GL}_2(\mathbb{Z})$

- $n = 2$, $\dim(V) = 3$, $\dim(V^{>0}/\mathbb{R}_{>0}) = 2$
- compute in affine section of the projective space
- $\mathcal{A}^{\geq 0} = \{ F \in V^{\geq 0} \mid \text{trace}(F) = 1 \}$
- $F_0 = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$, $\mu(F_0) = 2$, $\mathcal{M}(F_0) = \{ \pm (1, 0), \pm (0, 1), \pm (1, 1) \}$
- $\mathcal{A}^{\geq 0} \cap \text{Vor}(F_0) = \text{conv}(a = \begin{pmatrix} 10 \\ 00 \end{pmatrix}, b = \begin{pmatrix} 00 \\ 01 \end{pmatrix}, c = \frac{1}{2} \begin{pmatrix} 11 \\ 11 \end{pmatrix})$
Example, generators for $\text{GL}_2(\mathbb{Z})$

- Compute neighbor: $F_1 \in \mathcal{V}^{>0}$ so that $\text{Vor}(F_1) = \text{conv}(a, b, c')$.
- Linear equation on $F_1$: $\text{trace}(F_1a) = \text{trace}(F_1b) = 2$ and $\text{trace}(F_1c) > 2$,
- So $F_1 = F_0 + sX$ where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ generates $\langle a, b \rangle^\perp$.

- For $s = 2$ the matrix $F_1 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ has again 6 minimal vectors

- $\mathcal{M}(F_1) = \{ \pm(1, 0), \pm(0, 1), \pm(1, -1) \}$
- $\mathcal{A}^{>0} \cap \text{Vor}(F_1) = \text{conv}(a, b, c' := \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix})$
Example, generators for $\text{GL}_2(\mathbb{Z})$

$\triangleright \text{Stab}_{\text{GL}_2(\mathbb{Z})}(F_0) = \langle g = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle$

$\triangleright (a, b) \cdot g = (b, c), (b, c) \cdot g = (c, a)$

$\triangleright$ Compute isometry $t = \text{diag}(1, -1) \in \text{GL}_2(\mathbb{Z})$, so $t^{-1}F_0t^{-tr} = F_1$.  

$\triangleright$ Then $\text{GL}_2(\mathbb{Z}) = \langle g, h, t \rangle$. 

\[\begin{array}{c}
\text{Vor}(F_0) \\
\text{Vor}(F_1) \\
\end{array}\]
\( \text{GL}_2(\mathbb{Z}) = \langle g, h, t \rangle. \)

- \( \text{Stab}_{\text{GL}_2(\mathbb{Z})}(F_0) = \langle g = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle \)
- \((a, b) \cdot g = (b, c), (b, c) \cdot g = (c, a)\)
- Compute isometry \( t = \text{diag}(1, -1) \in \text{GL}_2(\mathbb{Z}), \) so \( t^{-1}F_0t^{-tr} = F_1. \)
Variations of Voronoi’s algorithm

- Many authors used this algorithm to compute integral homology groups of $\text{SL}_n(\mathbb{Z})$ and related groups, as developed C. Soulé in 1978.

- Max Köcher developed a general Voronoi Theory for pairs of dual cones in the 1950s. Let $\sigma : \mathcal{V}_1 \times \mathcal{V}_2 \rightarrow \mathbb{R}$ be non degenerate and positive on the cones $\mathcal{V}_{1 \times 0} \times \mathcal{V}_{2 > 0}$. A discrete admissible set $D \subset \mathcal{V}_{2 > 0}$ is used to define minimal vectors and perfection for $F \in \mathcal{V}_{1 > 0}$ and $\text{Vor}_D(F) \subset \mathcal{V}_{2 > 0}$.

- J. Opgenorth (2001) used Köcher’s theory to compute the integral normalizer $\mathcal{N}_{\text{GL}_n(\mathbb{Z})}(G)$ for a finite unimodular group $G$.

- M. Mertens (Masterthesis, 2012) applied Köcher’s theory to compute automorphism groups of hyperbolic lattices.

- This talk will explain how to apply it to obtain generators and relations for the unit group of orders in semi-simple rational algebras and an algorithm to solve the word problem in these generators.
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
- so $A_\mathbb{R}$ is isomorphic to a direct sum of matrix rings over of $\mathbb{H}$, $\mathbb{R}$ or $\mathbb{C}$.
- $A_\mathbb{R}$ carries a “canonical” involution $^\dagger$ (depending on the choice of the isomorphism) that we use to define symmetric elements:
  - $\mathcal{V} := \text{Sym}(A_\mathbb{R}) := \{ F \in A_\mathbb{R} \mid F^\dagger = F \}$
  - $\sigma(F_1, F_2) := \text{trace}(F_1 F_2)$ defines a Euclidean inner product on $\mathcal{V}$.
  - In general the involution $^\dagger$ will not fix the set $A$.

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

The discrete admissible set

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

\( L \)-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 \( F \).
- \( \mathcal{M}_L(F) := \{ \ell \in L \mid F[\ell] = \mu_L(F) \} \) the finite set of \( L \)-minimal vectors.
- \( \text{Vor}_L(F) := \{ \sum_{x \in \mathcal{M}_L(F)} a_x x^\dagger x \mid a_x \geq 0 \} \subset \mathcal{V}^{\geq0} \) Voronoi domain of \( F \).
- \( F \) is called \( L \)-perfect \( \Leftrightarrow \dim(\text{Vor}_L(F)) = \dim(\mathcal{V}) \).

Theorem

\( \mathcal{T} := \{ \text{Vor}_L(F) \mid F \in \mathcal{V}^>0, \ L \text{-perfect} \} \) forms a face to face tessellation of \( \mathcal{V}^{\geq0} \).
\( \Lambda^* \) acts on \( \mathcal{T} \) with finitely many orbits.
Generators for $\Lambda^*$

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

so here $\Lambda^* = \langle \text{Aut}(F_1), \text{Aut}(F_2), \text{Aut}(F_3), a, b, c, d, e, f \rangle$. 
Example \( \mathbb{Q}_{2,3} \).

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

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

Maximal order \( \Lambda = \langle 1, i, \frac{1}{2}(1 + i + ij), \frac{1}{2}(j + ij) \rangle \)

- \( V = A = \mathbb{Q}_{2,3}, A_\mathbb{R} = \mathbb{R}^{2 \times 2}, L = \Lambda \)

- Embed \( A \) into \( A_\mathbb{R} \) using the maximal subfield \( \mathbb{Q}[\sqrt{2}] \).

- Get three perfect forms:
  - \( F_1 = \begin{pmatrix} 1 & 2 - \sqrt{2} \\ 2 - \sqrt{2} & 1 \end{pmatrix}, F_2 = \begin{pmatrix} 6 - 3\sqrt{2} & 2 \\ 2 & 2 + \sqrt{2} \end{pmatrix} \)
  - \( F_3 = \text{diag}(-3\sqrt{2} + 9, 3\sqrt{2} + 5) \)
The tesselation for $\mathbb{Q}_{2,3} \leftrightarrow \mathbb{Q}[\sqrt{2}]^{2\times2}$.
\[ \Lambda^*/\langle \pm 1 \rangle = \langle a, b, t \mid a^3, b^2, atbt \rangle \]
Easy solution of the word problem
Easy solution of the word problem
Easy solution of the word problem

\[ \text{Pa} \quad \text{Pa}^{-1} \quad \text{PX} \]

\[ P \quad \text{Pa} \quad t \quad b \]
Easy solution of the word problem
The tessellation for $\mathbb{Q}_{2,3} \hookrightarrow \mathbb{Q}[\sqrt{3}]^{2 \times 2}$. 
Conclusion

- Algorithm works quite well for indefinite quaternion algebras over the rationals.
- Obtain presentation and algorithm to solve the word problem.
- For $Q_{19,37}$ 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 $\Lambda^*$, 431 perfect forms, 50 generators in about 10 minutes.
- Quaternion algebra with center $\mathbb{Q}[\zeta_5]$: > 40,000 perfect forms.
- Masterthesis by Oliver Braun: The tessellation $T$ can be used to compute the maximal finite subgroups of $\Lambda^*$.
- Masterthesis by Sebastian Schönnenbeck: Compute integral homology of $\Lambda^*$. 