AWS 2012

Generating $S$-arithmetic groups by small elements and small subgroups

T. Chinburg and M. Stover
Small Elements

§1. Pell equation

\[ x^2 - dy^2 = 1, \ x, y > 0, \ d > 0 \text{ square-free} \]

\((x_d, y_d) = \text{solution with minimal } x_d\)

\[ \log x_d = \# \text{ digits in } x_d \]

\[ \log d = \log \ d \]

Unknown: Is \( \log x_d \) bounded by a polynomial in \( \log d \)?

Expect No! \( \forall \varepsilon > 0 \), expect

I \( \infty \) many \( d \) so

\[ \log x_d > \frac{1}{2} - \varepsilon \]
why: \( x + y \sqrt{d} \in \mathcal{O}_k^* = \{ \pm \varepsilon_k \} \) \( \text{gcd} \)

\( k = \Theta(\sqrt{d}) \) units

\( \varepsilon_k > 1 \) fundamental

\[
\frac{x + y \sqrt{d}}{d} = \varepsilon_j \text{, } j \in \{1, 2, 3, 6\}
\]

\underline{Brauer-Siegel}: As \( d \to \infty \)

\[
\log \left( \frac{\ln \operatorname{Reg}(k)}{\log d \ln k} \right) \to 1
\]

Say \( \ln \operatorname{Reg}(k) \approx \sqrt{d} \)

where \( \operatorname{Reg}(k) = \log \varepsilon_k \)

\underline{Gauss conj.}: \( \varepsilon_k = 1 \) for positive proportion of \( k \).

Known only that \( \exists \ c > 0, \inf \)

many \( d \) so

\[
\log \varepsilon_k > (\log d \ln k)^c
\]
§2. Units + S-units

\[ k = \# \text{f1d} \geq \mathcal{O}_k \geq \mathcal{O}_k^* \]

\( H: k \to \mathbb{R} \) Height

\[ H(\alpha) = \prod \max(1, |\alpha|^1) \]

\( v \in V = \text{places of } k \)

E.g. \( k = \mathbb{Q}(\sqrt{d}), d > 0, H(\varepsilon_k) = \varepsilon_k \)

Expect: when \( k \) ranges over an infinite set of fields of given degree with infinite unit groups \( \mathcal{O}_k^* \), there is no polynomial in \( \text{Idr} / \mathcal{A} \) which bounds heights of some generating set for \( \mathcal{O}_k^* \).
Lenstra's Discovery (1990's)

S-units can be generated by elements of small height.

\[ V \supseteq S = \text{finite} \supseteq V_\infty = \text{arch. places} \]

\[ \mathcal{O}_{k,S} = \left\{ \alpha \in k : |\alpha|_v \leq 1 \text{ if } v \in V - S \right\} \]

\[ \mathcal{O}_{k,S} = \text{S-units} \]

\[ m_S = \max \left\{ \text{Norm}(v) : v \in S = \text{finite places in } S \right\} \]
Theorem (Lenstra) If $S$ contains all finite $v$ with $\text{Norm}(v) \leq \sqrt{1/2 \cdot \left(\frac{2}{\pi}\right)^2 z(k)}$

then $O^*_k, S$ is generated by elements of height

$\left(\frac{2}{\pi}\right)^{r_2(h)} \sqrt{1/2 \cdot \text{Id}_k} \in S$

(or: (Schoof) Find an algorithm for generating $O^*_k$ in poly. time in $\text{Id}_k^{1/2 + \varepsilon}$

Idea: $1 \rightarrow O^*_k \rightarrow O^*_k, S \rightarrow \mathbb{Q}_v \forall v \in S$
33. S units of division algebras

\[ B/k \text{ finite dim} \text{ } \text{div. alg.} \text{ center } k \]

\[ D = \mathcal{O}_k \text{ order in } B \]

\[ D_5 = \mathcal{O}_k, S \text{ and } \mathcal{O}_k D \supset \mathcal{O}_5 \]

1) Define an intrinsic height

\[ H: B^* \to \mathbb{R} \]

2) Define discriminant of \( D \)

3) Generalize Lenstra: If S moderately large

\[ S \text{ small generators of } D_5^* \]
One Application:

Find presentations for \( D_5^* \). Use these to study the congruence subgroup problem:
Does every finite index subgroup of \( D_5^* \) contain \( D_5^* \cap (1 + mD_5) \) for some integer \( m \)?

Generalizations?: \( B^* \) defines an alg. group \( G \subseteq GL_2(K) \) for which alg. gps \( G \) can \( G \langle (0_k, s) \rangle \) be generated by small height
14. Heights

\( v \in V = \text{places of } k \)

\( B_v = k_v \otimes_k B = \text{Mat}_{m(v)}(A_v) \)

\( A_v / k_v \text{ central div. alg.} \)

\( \dim_{k_v} A_v = d(v)^2 \)

\( m(v) d(v) = d, \quad d^2 = \dim_k B \).

Can make for almost all \( v \)

\( \mathcal{O}_v = \mathcal{O}_{k,v} \otimes_{\mathcal{O}_k} \text{Mat}_{m(v)}(U_v) \)

\( U_v = \text{max compact subgrp. of } A_v \)
\[ \text{det}_V : B_V \rightarrow k_V \]
\[ N_V : A_V \rightarrow k_V \]

reduced norms, from taking \( k_V \otimes k_V \) and then dets.

\[ Y_V = \left( \gamma_{ij}^V \right) \in B_V = \text{Mat}(A_V) \]

\[ |Y_V| = \max_V \left| N_V (\gamma_{ij}^V) \right| \]

Global Height: \( \gamma \in B^x \)

\[ y_V = \gamma \in B^x \]

\[ H(\gamma) = \prod_{V \in \mathcal{V}} \max \left( 1, |N_V (\gamma_{ij}^V)| \right) \]

= \prod_{V \in \mathcal{V}} \max \left( 1, \max_{i,j} \left| N_V (\gamma_{ij}^V) \right| \right) \]
35. Discriminants

For each:

\[ A_v = 1R \text{ has Euclidean Haar measure} \]

\[ A_v = 4 \text{ has } 2 \cdot (\ldots) \]

\[ A_v = H_{1R} = 1R + 1R^I + 1R^J + 1R^IJ \]

has 4. Euclidean H.M.

Gives Haar measure on

\[ B_{1R} = 1R \otimes B = \prod_{v \in V} \text{ Mat}_m(1R) \]

\[ \log = \text{covel} (B_{1R} / \mathcal{D}) \]

for \( \mathcal{D} = \text{Ok order in } B \).
§6. Theorem

There are functions $f_1(n, d)$ and $f_2(n, d)$ of $n = \lfloor k : Q \rfloor$ and $d = \sqrt{dm_n B}$ as follows. There's a max. order $D \subseteq B$ so that if $S$ contains all finite $V$ with $\text{Norm}(V) \leq f_2(n, s) \max(1, \text{cond}(Q))^c_1$, then $D$ is gen. by elements of height $< f_2(n, d) \max(1, \text{cond}(Q))^c_2$.$^{5f}$

Here $s > \# \sqrt{V \cap \mathcal{A}}$ with $A_V = H_R$. $c_1 = \frac{1}{d(n - \frac{s}{2})}$, $c_2 = \frac{2}{d + d}$, $c_3 = \frac{3n}{d(n - s/2)}$. 
37. Mechanism of Proof

Idea: Use Minkowski Thm to find many S-units of \( D \).

For \( x \in B \), let

\[
\text{Norm}_v(x) = \frac{\text{Norm}^v / Q_p(v)}{\det(v(x))} d
\]

\[
\text{Norm}_\infty(x) = \prod_{v \in V} \text{Norm}_v(x)
\]

for \( x = \prod_{v} x_v \)

\[
\text{Norm}_f(x) = \prod_{v \in V_f} \text{Norm}_v(x_v)
\]
\[ B^*_S = B^*_{IR} \times B^*_{Sf} \]
\[ B^*_{IR} = \prod_{v \in V_\infty} B^*_v, \quad B^*_{Sf} = \prod_{v \in S_f} B^*_v \]

\[ G_S = \{(x, \beta) : x \in B^*_{IR}, \beta \in B^*_{Sf}\} \]
\[ |\text{Norm}_{\omega_0}(x)| = \text{diag} \left( |\text{Norm}_f(\beta)|^{-1} \right) \]

Here

\[ \text{Norm}(x) \text{ and } \text{Norm}_f(\beta) \]

are in the ideals \( J(\Omega) \cap \mathbb{R} \).
Idea: Find a fundamental domain for the left multiplication action of $D^+_5$ on $G_5$.

$x \subseteq B^+_R \text{ convex, symmetric, compact} \implies \dim B = 3$

so $\text{vol}(x) \geq 2 \cdot \text{covol}(d\Theta)$

Choose $m_x \in \mathbb{R}$ so

$$\{ [x_v : \mathbb{R}] / \mathbb{R} \}$$

$$\| \text{Norm}_v (y_v) \|_v \leq m_x$$

for $v \in V \rightarrow$

$$y = (y_v)_v \in V \rightarrow \in X$$
\[ F_X = \{ (x, \beta) : \beta \in \mathcal{D} \in \mathcal{D}, \beta \mathcal{D} \subseteq \mathcal{D} \text{ where right } \mathcal{D} \text{ ideal}, \] \[ L \mathcal{D} : \beta \mathcal{D} \leq \mathcal{m}_X \} \]

Prop: If \( S \) contains all \( \nu \) of \( k \) with \( \| \text{Norm}_{k/\mathcal{D}}(\nu) \|_{\mathbf{d}} \leq \mathcal{m}_X \) then \( \mathcal{D}_S^* \cdot F_X = \mathcal{C}_S \). So \( F_X \) contains a fundamental domain for the action of \( \mathcal{D}_S^* \) on \( \mathcal{C}_S \).
Idea of Proof

Use Minkowski to show that for all \((x, \beta) \in G\), there is a \(c \in D_\beta^+\) so \((cx, c\beta) \in F_x\).

Look for \(c \in D_\beta^+ \cap (F_x - 1)\) lattice convex symmetric.

Show \(c \in D_\beta^+\) by bounding norms.
Topological Lemma:

A set of $P = \text{topological generators}$ for $G_S$.

So $\langle P, \text{any nonempty } \rangle = G_S$ open.

Suppose $P = P^{-1}$ as sets.

Lemma: $D_S$ generated by its intersection with $F_X P F_X^{-1}$.

Application: Choose $P$ with small heights, bound heights of elts of $D_S^+ \wedge F_X P F_X^{-1}$.
Idea of Proof of Lemma

$\Delta = \text{group gen. by}$

$D^*_s \cap F_x \cdot P \cdot F_x^{-1}$

Show $\Delta F_x$ stable by right mult. by any $z \in P$:

$y \cdot z \in F_x \cdot P$

$= y \cdot x$

For some $y \in D^*_s$, $x \in F_x$, since $D^*_s F_x = G_s$. Then

$x = y \cdot x' \in F_x \cdot P \cdot F_x^{-1}$

so $y \in \Delta$ any $F_x \cdot P \subseteq \Delta x$

Then $\Delta F_x \cdot P = \Delta \ast F_x = G_s$

since $P = \text{top. generators}$
Now we could have used this argument after shrinking $F_x$ to a fundamental domain $F'_x$ for the action of $\Theta'_s$ (leaving $\Delta$ as before). bijective

Then $\Theta'_s \times F'_x \to G_s$

$(x, u) \to \tau u$

$\Delta \times F'_x \to G_s$

subjective

$\Delta \trianglelefteq \Theta'_s \implies \Delta = \Theta'_s \ast$. 