AWS 2012

Generating S-arithmetic groups by small elements and small subgroups

T. Chinburg and M. Stover

Small Elements

§1. Pell equation

$x^2 - dy^2 = 1$, $x, y > 0$, $d > 0$ $\square$-free

(x_d, y_d) = solution with minimal x_d

$\log x_d$ = # digits in x_d

$\log d$ = " " d

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

Expect No! $\forall \varepsilon > 0$, expect $\exists \infty$ many d so

$$\log x_d > d^{1/2 - \varepsilon}$$

(3)

Why: $x + y\sqrt{d} \in \mathcal{O}_k^* = \{\pm \varepsilon_k^n\}_{n \in \mathbb{Z}}$

$k = \mathbb{Q}(\sqrt{d})$ $\quad$ $\parallel$ units

$\varepsilon_k > 1$ fundamental

$x_d + y_d\sqrt{d} = \varepsilon_k^j, \quad j \in \{1, 2, 3, 6\}$

Brauer-Siegel As $d \to \infty$

$$\frac{\log(h_k \operatorname{Reg}(k))}{\log d_k^{1/2}} \to 1$$

Say $\quad h_k \operatorname{Reg}(k) \approx d_k^{1/2}$

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

Gauss Conj. $h_k = 1$ for positive proportion of k.

Known only that $\exists\, c > 0$, inf. many d so

$$\log \varepsilon_k > (\log d_k)^c$$

§2. Units + S-units

$k = \#\text{ fld} \supseteq \mathcal{O}_k \supseteq \mathcal{O}_k^*$

$H : k \to \mathbb{R}$ Height

$$H(\alpha) = \prod_{v \in V} \max(1, |\alpha|_v)$$

$v \in V$ = 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 $|d_{k/\mathbb{Q}}|$ which bounds heights of some generating set for $\mathcal{O}_k^*$.

<u>Lenstra's Discovery</u> (1990's)

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

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

$$O_{k,S} = \left\{ \alpha \in k : |\alpha|_v \leq 1 \text{ if } v \in V - S \right\}$$

$\cup$

$O_{k,S}^* =$ S-units

$$m_S = \max \left\{ \text{Norm}(v) : v \in S_f = \text{finite places in } S \right\}$$

<u>Thm</u> (Lenstra) If S contains all finite v with $\text{Norm}(v) < |d_k|^{1/2} \left(\frac{2}{\pi}\right)^{r_2(k)}$ then $O_{k,S}^*$ is generated by elements of height

$$< \left(\frac{2}{\pi}\right)^{r_2(k)} |d_k|^{1/2} m_S$$

<u>Cor:</u> (Schoof) $\exists$ an algorithm for generating O_k^* in poly. time in $|d_k|^{1/2+\varepsilon}$

1^{st} <u>Idea</u>: $1 \to O_k^* \to O_{k,S}^* \to \bigoplus_{v \in S_f} \mathbb{Z}$

§3. S units of division algebras

B/k finite dim'l div. alg. center k

$\mathcal{D} = \mathcal{O}_k$ order in B

$\mathcal{D}_S = \mathcal{O}_{k,S} \otimes_{\mathcal{O}_k} \mathcal{D} \supseteq \mathcal{D}_S^*$

1) Define an intrinsic height
$H : B^* \to \mathbb{R}$

2) Define discriminant $d_{\mathcal{D}}$

3) Generalize Lenstra: If S moderately large, $\exists$ small generators of $\mathcal{D}_S^*$

<u>One Application</u>:

Find Presentations for $\mathcal{O}_S^*$. Use these to study the <u>congruence subgroup problem</u>: Does every finite index subgroup of $\mathcal{O}_S^*$ contain $\mathcal{O}_S^* \cap (1 + m\,\mathcal{O}_S)$ for some integer m?

<u>Generalizations?</u>: B^* defines an alg. group $G \leq GL_2(k)$

For which alg. gps G can $G(\mathcal{O}_{k,S})$ be generated by elts of <u>small height</u>

§4. Heights

$v \in V =$ places of k

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

A_v / k_v central div. alg.

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

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

Can make for almost all v

$$\mathcal{D}_v = \mathcal{O}_{k,v} \otimes_{\mathcal{O}_k} \mathcal{D} \leq \mathrm{Mat}_{m(v)}(U_v)$$

$U_v =$ max compact subgp. of A_v

$$\det_v : B_v \to k_v$$

$$N_v : A_v \to k_v$$

reduced norms, from taking $\bar{k}_v \otimes_{k_v}$ and then dets.

$$\gamma_v = (\gamma_v^{i,j})_{i,j} \in B_v = \mathrm{Mat}(A_v)$$

$$|\gamma_v|_v = \max_{i,j} |N_v(\gamma_v^{i,j})|_v^{\frac{1}{d(v)}}$$

<u>Global Height</u>: $\gamma \in B^*$

$$\downarrow$$

$$\gamma_v = \gamma \in B_v^*$$

$$H(\gamma) = \prod_{v \in V} \max(1, |\gamma_v|_v^{d(v)})$$

$$= \prod_{v \in V} \max(1, \max_{i,j} |N_v(\gamma_v^{i,j})|_v)$$

§5. Discriminants

For v arch:

$A_v = \mathbb{R}$ has Euclidean Haar measure

$A_v = \mathbb{C}$ has $2 \cdot$ (")

$A_v = \mathbb{H}_{\mathbb{R}} = \mathbb{R} + \mathbb{R}I + \mathbb{R}J + \mathbb{R}IJ$ has $4 \cdot$ Euclidean H.M.

Gives Haar measure on

$$B_{\mathbb{R}} = \mathbb{R} \otimes_{\mathbb{Q}} B = \prod_{v \in V_\infty} \mathrm{Mat}_{m(v)}(A_v)$$

$$d_{\mathcal{D}} = \mathrm{covol}(B_{\mathbb{R}} / \mathcal{D})$$

for $\mathcal{D} = \mathcal{O}_k$ order in B.

§6. Theorem

There are functions $f_1(n, d)$ and $f_2(n, d)$ of $n = [k : \mathbb{Q}]$ and $d = \sqrt{\dim_k B}$ as follows.
There's a max. order $\mathcal{D} \subseteq B$ so that if S contains all finite v with

$$\mathrm{Norm}(v) \leq f_1(n, s)\max(1, \mathrm{covol}(\mathcal{D})^{c_1})$$

then $\mathcal{D}_S^*$ gen. by elements of Height

$$< f_2(n, d)\, m_{S_f}^{c_2} \max\left(1, \mathrm{covol}(\mathcal{D})^{c_3}\right)$$

Here $s = \#\, v \in V_\infty$ with $A_v = H_{\mathbb{R}}$

$c_1 = \dfrac{1}{d(n - \frac{s}{2})}$; $c_2 = \dfrac{2}{d} + d$; $c_3 = \dfrac{3n}{d(n - s/2)}$.

§7. Mechanism of Proof

Idea: Use Minkowski Thm to find many S-units of $\mathcal{D}$.

For $x_v \in B_v$ let

$$\mathrm{Norm}_v(x_v) = \mathrm{Norm}_{k_v/\mathbb{Q}_{p(v)}} \det_v(x_v)^d$$

$$\mathrm{Norm}_\infty(x) = \prod_{v \in V_\infty} \mathrm{Norm}_v(x_v)$$

for $x = \prod_v x_v$

$$\mathrm{Norm}_f(x) = \prod_{v \in V_f} \mathrm{Norm}_v(x_v)$$

$$B_S^* = B_{\mathbb{R}}^* \times B_{S_f}^*$$

$$B_{\mathbb{R}}^* = \prod_{v \in V_\infty} B_v^* \; ; \; B_{S_f}^* = \prod_{v \in S_f} B_v^*$$

$$G_S = \left\{ (x, \beta) : x \in B_{\mathbb{R}}^*, \ \beta \in B_{S_f}^*, \ |\mathrm{Norm}_\infty(x)| = |\mathrm{Norm}_f(\beta)|^{-1} \right\}$$

$$\Big\uparrow \text{diag.}$$

$$\mathcal{D}_S^*$$

Here

$\mathrm{Norm}_\infty(x)$ and $\mathrm{Norm}_f(\beta)$

are in the ideles $J(\mathbb{Q})$

$$J(\mathbb{Q}) \xrightarrow{|\ |} \mathbb{R}.$$

<u>Idea</u>: Find a fundamental domain for the left multiplication action of $\mathcal{D}_S^*$ on G_S.

$X \subseteq B_{\mathbb{R}}$ convex, symmetric, compact

so $\mathrm{vol}(X) \geqslant 2^{\dim_{\mathbb{Q}} B} \mathrm{covol}(\mathcal{D})$

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

$$|\mathrm{Norm}_v(y_v)|_v^{[k_v:\mathbb{R}]/n} \leq m_X$$

for $v \in V_\infty$

$$y = (y_v)_{v \in V_\infty} \in X$$

$$F_X = \left\{ (x, \beta) : \begin{array}{l} x \in X \, ; \\ \beta\mathcal{D} \subseteq \mathcal{D} \text{ where } \beta\mathcal{D} = \text{right } \mathcal{D} \text{ ideal} \, ; \\ [\mathcal{D} : \beta\mathcal{D}] \leq m_X \end{array} \right\}$$

<u>Prop:</u> If S contains all v of k with $|\mathrm{Norm}_{k/\mathbb{Q}}(v)|^d \leq m_X$

then

$$\mathcal{D}_S^* \cdot F_X = G_S$$

so F_X contains a fundamental domain for the action of $\mathcal{D}_S^*$ on G_S

Idea of Proof

Use Minkowski to show that for all $(x, \beta) \in G_S$ there is a $c \in \mathcal{O}_S^*$ so $(cx, c\beta) \in F_X$

Look for $c \in \underbrace{\mathcal{O}\beta^{-1}}_{\text{lattice}} \cap \underbrace{(F_X x^{-1})}_{\substack{\text{convex}\\ \text{symmetric}}}$

Show $c \in \mathcal{O}_S^*$ by bounding norms

Topological Lemma:

$\underline{P}$ = a set of topological generators for G_S

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

Suppose $\underline{P} = \underline{P}^{-1}$ as sets

Lemma: $\mathcal{D}_S^*$ generated by its intersection with

$F_X \underline{P} F_X^{-1}$.

Application: Choose $\underline{P}$ with small heights, bound heights of elts of $\mathcal{D}_S^* \cap F_X \underline{P} F_X^{-1}$

Idea of Proof of Lemma

Δ = group gen. by

$$\mathcal{D}_S^{*} \cap F_x \, \underline{P} \, F_x^{-1}$$

Show ΔF_x stable by right mult. by any $\tau \in \underline{P}$:

$$y \cdot \tau \in F_x \cdot \underline{P}$$
$$\parallel$$
$$\gamma \cdot x$$

For some $\gamma \in \mathcal{D}_S^{\bullet}$, $x \in F_x$, since $\mathcal{D}_S^{\bullet} F_x = G_S$. Then

$$\gamma = y \tau x^{-1} \in F_x \cdot \underline{P} \cdot F_x^{-1}$$

So $\gamma \in \Delta$ any $F_x \cdot \underline{P} \subseteq \Delta x$

Then $\Delta F_x \underline{P} = \Delta F_x = G_S$ since $\underline{P}$ = top. generators

Now we could have used this argument after shrinking F_x to a fundamental domain F_x' for the action of $\mathcal{D}_S'$ (leaving Δ as before).

Then

$$\mathcal{D}_S^* \times F_x' \xrightarrow{\text{bijective}} G_S$$

$$(\gamma, u) \to \gamma u$$

$$\Delta \times F_x' \xrightarrow[\text{surjective}]{} G_S$$

$$\Delta \subseteq \mathcal{D}_S^* \Rightarrow \Delta = \mathcal{D}_S^*.$$