Small generators for S-unit groups II

Ted Chinburg Matthew Stover

Today: B = quaternion algebra / $\mathbb{Q}$

$\mathcal{O}$ a $\mathbb{Z}$-order of B

$S = \{\infty, p_1, \ldots, p_r\}$ a finite set of places $\supseteq \{\infty\}$

Goal: Find generators of $\mathcal{O}_S^*$ of small height.

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

$$|\gamma|_v = \max_{i,j} \{|\gamma^{i,j}(v)|_v\}$$

$$\gamma^{i,j}(v) = \rho_v(\gamma), \quad \rho_v(\gamma) \in B_v \cong \begin{cases} A_v & d(v) = 2 \\ M_2(\mathbb{Q}_v) & d(v) = 1 \end{cases}$$

On a $\mathbb{Q}_v$-algebra A_v (division):

$$|x|_v = |N_v(x)|^{1/d(v)} \quad (v \text{ archimedean})$$

$$|N_v(\lambda_v)|^{1/d(v)} \quad (v \text{ nonarch. } = \lambda_v)$$

$$\hookrightarrow = (\# k(v))^{-1/d(v)}$$

uniformiz.

$$B_{\mathbb{R}} \cong \begin{cases} \mathbb{H} \\ M_2(\mathbb{R}) \end{cases}$$

Haar measure on $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}I \oplus \mathbb{R}J \oplus \mathbb{R}IJ \cong \mathbb{R}^4$

is $4\, dx_1 dx_2 dx_3 dx_4$

Standard measure on $\mathbb{R}$, product measure on $M_2(\mathbb{R}) \cong \mathbb{R}^4$

$\Rightarrow \mathcal{O} \hookrightarrow B_{\mathbb{R}}$ as a lattice of covolume

$|d_{\mathcal{O}}|$ = <u>discriminant</u> of $\mathcal{O}$.

(both are defined via $(\mathrm{Tr}(\alpha_i \alpha_j))_{i,j}$).

<u>Want</u>: Convex symmetric subset of $B_{\mathbb{R}}$.

$\mathbb{H}$ $\quad |x| = |N(x)|^{1/2}$, N = reduced norm

$\mathbb{R}$ $\quad |x| = |x|$, $\quad |\gamma| = \max_{i,j} |\gamma_{i,j}|$, $\gamma \in M_2(\mathbb{R})$.

Let $X(c) = \{ x \in B_{\mathbb{R}} : |x|^{d(v)} \leq c \}$

$$\Rightarrow \mathrm{Vol}(X(c)) = \begin{cases} 16c^4 & B_{\mathbb{R}} \cong M_2(\mathbb{R}) \\ 2\pi^2 c^2 & B_{\mathbb{R}} \cong \mathbb{H} \end{cases}$$

Choose c such that

$$\mathrm{Vol}(X(c)) = 2^{\dim_{\mathbb{Q}} B} \cdot d_{\mathcal{D}} = 16 d_{\mathcal{D}}$$

$$\Rightarrow \quad c = \begin{cases} \sqrt[4]{d_{\mathcal{D}}} & B_{\mathbb{R}} \cong M_2(\mathbb{R}) \\ \frac{2\sqrt{2}}{\pi} \sqrt{d_{\mathcal{D}}} & B_{\mathbb{R}} \cong \mathbb{H} \end{cases}$$

Want m_X so that $|N_\infty(y)|^{d(v)} \leq m_X$ for all $y \in X(c)$

$$\Rightarrow \quad m_X = \begin{cases} 2c^2 & B_{\mathbb{R}} \cong M_2(\mathbb{R}) \\ \sqrt{c} & B_{\mathbb{R}} \cong \mathbb{H} \end{cases}$$

Let S be a finite set of places

$$F_{X(c)} = \{ (x,\beta) \in G_S : x \in X(c),\ \beta\mathcal{O} \subseteq \mathcal{O},\ [\mathcal{O} : \beta\mathcal{O}] \leq m_X \}$$

$$G_S = \{ (x,\beta) \in B_{\mathbb{R}}^* \times \prod_{v \in S \setminus \{\infty\}} B_v^* : \text{product formula holds} \}$$

<u>Prop$^{\underline{n}}$</u> If S contains all finite places of $\mathbb{Q}$ with $\mathrm{Norm}(v)^2 \leq m_X$, then $F_{X(c)}$ is a fundamental domain for $\mathcal{O}_S^*$ acting on G_S.

$P = \{\text{topological generators for } G_S\}$
$\iff \langle P, O \rangle = G_S$ for all $O \subset G_S$ open.
Work place by place.

$B_{\mathbb{R}}^* \cong GL_2(\mathbb{R}) \Rightarrow 2$ connected components (sign(det))

Any open subset generates $GL_2^+(\mathbb{R})$

$\Rightarrow$ need $\left(\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, 1, 1, \ldots, 1 \right) \in G_S$.

$\mathbb{H}$ is connected, so we take the identity.

$B_v^* \cong GL_2(\mathbb{Q}_v)$, v non archimedean, can take elementary matrices with $\mathbb{Z}_v^*$ entries, permutation matrices, and

$$\begin{pmatrix} \pi_v^{\pm 1} & 0 \\ 0 & 1 \end{pmatrix}$$

$$\Rightarrow \sup \left\{ 1, |z_v|_v^{d(v)}, z = \prod_v z_v \in P \right\} \leq \sqrt{\max_{p \in S} \{p\}}$$

C

<u>Lemma</u> $\mathcal{D}_S^*$ is generated by $\mathcal{D}_S^* \cap F_X P F_X^{-1}$.

<u>Claim</u>: Every element of $\mathcal{D}_S^* \cap F_X P F_X^{-1}$ has height bounded by

$$\left[\left(2c^2\sqrt{m_{S_f}}\sqrt{m_X}\right)\left(\frac{1}{2}\right)^s\right] \times \left[m_{S_f}^2\sqrt{m_X}\right]$$

$$s = \#\mathrm{Ram}_\infty(B)$$

$$m_{S_f} = \max\{p : p \in S \setminus \{\infty\}\}$$

Idea of the proof.

Consider $(\gamma, \gamma) = (x_\infty z_\infty y_\infty^{-1}, \alpha_f \delta_f \beta_f^{-1})$

with $(x_\infty, \alpha_f), (y_\infty, \beta_f) \in F_X$

$(z_\infty, \delta_f) \in P$.

$W(\gamma) = W_\infty(\gamma) \cup W_f(\gamma) = \{ v \in S : |\gamma|_v > 1 \}$

$$H(\gamma) = \prod_{v \in W_\infty(\gamma)} |x_v z_v y_v^{-1}|_v^{d(v)} \times \prod_{v \in W_f(\gamma)} |\alpha_v \delta_v \beta_v^{-1}|_v^{d(v)}$$

$$= \prod_{v \in W_\infty(\gamma)} |x_v z_v \det_v(y_v) y_v^{-1}|_v^{d(v)}$$

$$\times \prod_{v \in W_f(\gamma)} \left(|\det_v(\beta_v)| \cdot |\alpha_v \delta_v \beta_v^{-1}|_v^{d(v)} \right)$$

$$\times \prod_{v \in W_\infty(\gamma)} |\det_v(y_v)|_v^{-1}$$

$$\times \prod_{v \in W_f(\gamma)} |\det_v(\beta_v)|_v^{-1}$$

Now study and bound each term.

Ex: $B = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \mathbb{Q} \oplus \mathbb{Q}I \oplus \mathbb{Q}J \oplus \mathbb{Q}IJ$

$I^2 = J^2 = -1, \quad IJ = -JI.$

$\mathrm{Ram}(B) = \{\infty, 2\}$

$\mathcal{O} = \mathbb{Z}[I, J, \alpha], \quad \alpha = \frac{1+I+J+IJ}{2}$

$=$ Hurwitz order

$d_{\mathcal{O}} = 2.$

$X(c) = \{ v \in \mathbb{R}^4 : \|v\| \leq \sqrt{c} \}$, $\mathbb{R}^4$ w/ basis $\{1, I, J, IJ\}$

(reduced norm = square of Euclidean length)

$\Rightarrow \mathrm{Vol}(X(c)) = 2\pi^2 c^2 \geq 16\, d_{\mathcal{O}} = 32$

$\Rightarrow c = 4/\pi$

$\Rightarrow m_X = 16/\pi^2.$

Must assume S contains all rational primes p such that $p^2 \le m_X \Rightarrow p \le 4/\pi < 2$

$\Rightarrow$ we can take $S = \{\infty\}$ and we find generators for $\mathcal{D}^*$!

Height bound is $\dfrac{256}{\pi^4} < 2.63$

Short computation returns

$$\left\{ \pm 1, \pm I, \pm J, \pm IJ, \frac{\pm 1 \pm I \pm J \pm IJ}{2} \right\} = \mathcal{D}^*$$

= binary tetrahedral group.

$S = \{\infty, 3\}$

Height bound becomes $\left(3^{3/2}\right)\left(\frac{256}{\pi^4}\right) < 13.66$

$\Rightarrow$ elements of $\mathcal{O}_S^*$ satisfying this bound lie in $\frac{1}{9}\mathcal{O}$

$\Rightarrow$ need to consider

$$V_{a,b,c,d,n} = 3^{-n}(a + bI + cJ + d\alpha)$$

$a, b, c, d \in \mathbb{Z}$, $0 \leq n \leq 2$

such that $|V_{a,b,c,d,n}|_\infty < (13.66)\, 3^n$.

Can be more efficient, but only slightly so, using the geometry of the Bruhat-Tits tree of $PGL_2(\mathbb{Q}_3)$.

$S = \{\infty, l_1, \ldots, l_n\}$

$l_1 < l_2 < \cdots < l_n$. distinct primes.

$\Rightarrow$ height bound is $\frac{256}{\pi^4} l_n^{3/2}$

Can show $\mathcal{D}_S^*$ is generated by

- $\{l_i\}_{i=1}^n$
- $\{\gamma \in \mathcal{D} : N(\gamma) \in \{1, l_1, \ldots, l_n\}\}$

Possible application: Experiment with congruence subgroup property.

Ex: $PSL_2(\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/3\mathbb{Z})$

Lots of finite index subgroups:

$$K_N = \text{kernel}\left(\rho_N : PSL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z}/N\mathbb{Z})\right)$$

(and pullbacks of subgroups of $PSL_2(\mathbb{Z}/N\mathbb{Z})$).

Question: Are these all of them?

No: A_5 is generated by elements of orders 2 and 3 $\Rightarrow \exists\, \rho : PSL_2(\mathbb{Z}) \to A_5$, but A_5 is never a subgroup of $PSL_2(\mathbb{Z}/N\mathbb{Z})$.

G an algebraic group $/ R$

$\Rightarrow$ homomorphism $\widehat{G(R)} \to G(\hat{R})$

$$\widehat{PSL_2(\mathbb{Z})} \longrightarrow PSL_2(\hat{\mathbb{Z}})$$

Is this kernel trivial? (or finite?)

For $SL_n(\mathbb{Z})$, $n \geq 3$, the answer is <u>yes</u>

(Bass-Milnor-Serre, Mennicke, ...)

$\Rightarrow$ number theory sees all the geometry of finite sheeted coverings of the space

$$SL_n(\mathbb{Z}) \backslash SL_n(\mathbb{R}) / SO(n).$$

Serre $SL_2(\mathcal{O}_S)$

$\mathcal{O}$ = ring of integers of k = # field

has CSP $\iff |S| \geq 2$ $(S \supseteq V_\infty$ = arch. places$)$

not CSP : $SL_2(\mathbb{Z})$, $SL_2(\mathcal{O}_{-d}) \leftarrow k = \mathbb{Q}(\sqrt{-d})$

= lattices in $SL_2(\mathbb{R})$ or $SL_2(\mathbb{C})$.

CSP : $SL_2(\mathbb{Z}[1/p])$, $SL_2(\mathbb{Z}[\sqrt{d}])$ $d > 0$.

Quaternion algebras. B/k

① $S = \{\text{all archimedean places}\}$ and $\mathrm{Ram}_\infty(B) =$ all but one place $\Rightarrow$ CSP fails (Fuchsian & Kleinian groups = lattices in $SL_2(\mathbb{R})$ or $SL_2(\mathbb{C})$).

② $\mathrm{Ram}_\infty(B) =$ all archimedean places

$S = \{\infty_1, \ldots, \infty_n, \mathfrak{p}\} \Rightarrow$ CSP fails.

(lattice in $SL_2(\mathbb{Q}_p) \Rightarrow$ virtually free group)

Ihara

Nothing else is known.

Note These are the cases where

$$\#(S \setminus \mathrm{Ram}_\infty(B)) = 1.$$

<u>Fact.</u> $G/\mathbb{Q}$ algebraic, semisimple

Suppose $G(\mathbb{Z}) \to \mathbb{Z}$.

Then CSP fails.

$$\text{CSP} \Leftrightarrow G(\hat{\mathbb{Z}}) \cong \widehat{G(\mathbb{Z})}$$

$$G(\mathbb{Z}) \to \mathbb{Z} \Rightarrow \widehat{G(\mathbb{Z})} \to \hat{\mathbb{Z}}$$

but $G(\hat{\mathbb{Z}})$ is a product of $G(\mathbb{Z}_p)$ and

$$G(\mathbb{Z}_p) \not\to \hat{\mathbb{Z}}.$$

$$\Rightarrow \widehat{G(\mathbb{Z})} \to G(\hat{\mathbb{Z}}) \text{ has } \underline{\text{huge}} \text{ kernel.}$$