Presentations for quaternionic S-unit groups

Ted Chinburg[1], Holley Friedlander[2], Sean Howe[3], Michiel Kosters[4], Bhairav Singh[5], Matthew Stover[6], Ying Zhang[7], and Paul Ziegler[8]

[1]University of Pennsylvania , ted@math.upenn.edu
[2]Williams College , hf2@williams.edu
[3]University of Chicago , seanpkh@gmail.com
[4]Universiteit Leiden , mkosters@math.leidenuniv.nl
[5]MIT , bsingh@mit.edu
[6]Temple University, mstover@temple.edu
[7]University of Iowa, ying-zhang-1@uiowa.edu
[8]ETH Zurich , paul.ziegler@math.ethz.ch

October 14, 2014

1 Introduction and notation

In this paper, we give an algorithm for presenting S-unit groups of an order $\mathcal{O}$ in a definite rational quaternion algebra B such that, for every $p \in S$ at which B splits, the localization of $\mathcal{O}$ at p is maximal and all left ideals of $\mathcal{O}$ of norm p are principal. We then apply this to give presentations for projective S-unit groups of the Hurwitz order in Hamilton's quaternions over the rational field $\mathbb{Q}$. To our knowledge, this provides the first explicit presentations of an S-arithmetic lattice in a semisimple Lie group with S large. We also include some discussion and experimentation related to the congruence subgroup problem, which is open for S-units of the Hurwitz order when S contains at least two odd primes.

We now introduce the objects studied in this paper, assuming some familiarity with the theory of quaternion algebras over number fields, e.g., from [10]. Let B denote a definite quaternion algebra over $\mathbb{Q}$ and $\mathcal{O} \subset B$ an order, that is, a $\mathbb{Z}$-order of full rank. Tensoring over the real numbers, we have $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}$, where $\mathbb{H}$ denotes Hamilton's quaternions. For each prime p, let $B_p = B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ be the completion of B at p. When p splits B,

suppose that $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is a maximal order of B_p, and we fix an isomorphism $B_p \cong \mathrm{M}_2(\mathbb{Q}_p)$ that identifies $\mathcal{O}_p$ with $\mathrm{M}_2(\mathbb{Z}_p)$. Let N denote the reduced norm on B.

Throughout this paper, $\mathcal{H}$ will denote the rational quaternion algebra with basis $\{1, I, J, IJ\}$ subject to the relations

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

Let $\mathcal{M}$ denote the *Hurwitz order* of $\mathcal{H}$, i.e., the maximal $\mathbb{Z}$-order with basis

$$\left\{1,\ I,\ J,\ \frac{1}{2}(1 + I + J + IJ)\right\}.$$

The algebra $\mathcal{H}_2$ is isomorphic to the unique quaternion division algebra over $\mathbb{Q}_2$ with unique maximal $\mathbb{Z}_2$-order $\mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Z}_2$. For odd p, $B_p \cong \mathrm{M}_2(\mathbb{Q}_p)$, and we fix an isomorphism as above such that $\mathcal{M}$ maps to $\mathrm{M}_2(\mathbb{Z}_p)$. The reduced norm on $\mathcal{H}$ is given by

$$\mathrm{N}(a + bI + cJ + dIJ) = a^2 + b^2 + c^2 + d^2.$$

For any finite, possibly empty, set of rational primes S, set $\mathbb{Z}_\emptyset = \mathbb{Z}$ and for $S = \{p_1, \ldots, p_r\}$ the *S-integers* are

$$\mathbb{Z}_S = \mathbb{Z}\left[\frac{1}{p_1}, \ldots, \frac{1}{p_r}\right].$$

Also, set

$$m_S = \prod_{p \in S} p.$$

For any B, $\mathcal{O}$ as above, let $\mathcal{O}_S$ be the *S-order* $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_S$. For any such S, Γ_S will denote the *S-unit group* $\mathcal{O}_S^*$ of invertible elements in the ring $\mathcal{O}_S$. It is well-known that $\mathcal{M}^*$ is the binary tetrahedral group [10, §V.3. A], which is also isomorphic to the group $\mathrm{SL}_2(\mathbb{F}_3)$.

To find presentations for Γ_S (more precisely, the group $\overline{\Gamma}_S$ of S-units modulo scalars), we study the discrete action of Γ_S on a product of *Bruhat–Tits trees*. For any prime $p \in S$ with $B_p \cong \mathrm{M}_2(\mathbb{Q}_p)$, let $\mathfrak{X}_p$ be the Bruhat–Tits tree associated with $\mathrm{PGL}_2(\mathbb{Q}_p)$. See [8, II §1] for the construction of $\mathfrak{X}_p$. For the remaining $p \in S$, let $\mathfrak{X}_p$ be a single point with trivial action by B_p^*. For S as above, define

$$\mathfrak{X}_S = \prod_{p \in S} \mathfrak{X}_p.$$

Under the homomorphism

$$\alpha_S : \Gamma_S \to \prod_{p \in S} B_p^*$$

we obtain an action of Γ_S on $\mathfrak{X}_S$ via our chosen isomorphism between B_p^* and $\mathrm{GL}_2(\mathbb{Q}_p)$ and the natural action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on $\mathfrak{X}_p$. It is well known that this action is discrete and cocompact, i.e., the natural simplicial structure on $\mathfrak{X}_S$ coming from the trees $\mathfrak{X}_p$ makes $\Gamma_S \backslash \mathfrak{X}_S$ a finite CW complex. (This is also clear from Theorem 2.1 below.) Note that the scalars in Γ_S act trivially, so the Γ_S action factors through the projection onto $\overline{\Gamma}_S$.

Acknowledgments

We thank the organizers of the 2012 Arizona Winter School, where this work began. This material is based upon work supported by the National Science Foundation under Grant Numbers NSF 0943832 and 1361000 and the National Science Foundation Graduate Research Fellowship Program under Grant No. DGE-1144082.

2 A fundamental domain and the basic algorithm

Let B denote a definite rational quaternion algebra, $\mathcal{O} \subset B$ an order, S a finite set of rational primes, and $\overline{\Gamma}_S$ the associated projective unit group. When $p \in S$ splits B, we assume that $\mathcal{O}_p$ is maximal, and fix an isomorphism $\mathcal{O}_p \to \mathrm{M}_2(\mathbb{Z}_p)$. Our presentation for $\overline{\Gamma}_S$ depends on finding a nice fundamental domain for its action on $\mathfrak{X}_S$. By a *vertex* of $\mathfrak{X}_S$, we will always mean a product of vertices of the factors. If x is a vertex of $\mathfrak{X}_p$, let $N(x)$ be the set of neighboring vertices. If $v = (v_p)_{p \in S}$ is a vertex of $\mathfrak{X}_S$, let $N(v) = \prod N(v_p)$.

For each $p \in S$ at which B splits, let $v_{0,p}$ be the vertex of the tree $\mathfrak{X}_p$ associated with the standard lattice

$$\mathcal{L}_{0,p} = \mathbb{Z}_p \oplus \mathbb{Z}_p. \tag{1}$$

Under the action of $B_p^* = \mathrm{GL}_2(\mathbb{Q}_p)$ on $\mathfrak{X}_p$, $v_{0,p}$ is stabilized by

$$(\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^* \cdot \mathbb{Q}_p^* = \mathrm{GL}_2(\mathbb{Z}_p) \cdot \mathbb{Q}_p^*.$$

For the remaining p in S, let $v_{0,p}$ be the unique vertex of $\mathfrak{X}_p$. Our fundamental domain is an open neighborhood of the vertex $v_0 = (v_{0,p})_{p \in S}$ in $\mathfrak{X}_S$.

Note that the stabilizer of v_0 in Γ_S is $\mathcal{O}^* \cdot \mathbb{Z}_S$. Our algorithm for presenting $\overline{\Gamma}_S$ is based on the following theorem.

Theorem 2.1. *Let B be a definite rational quaternion algebra and $\mathcal{O} \subset B$ be an order. Suppose that S is a finite set of primes such that, for every $p \in S$ at which B splits, the localization $\mathcal{O}_p$ of $\mathcal{O}$ at p is a maximal order of B_p and all left ideals of $\mathcal{O}$ of norm p are principal. Then the action of Γ_S (hence of $\overline{\Gamma}_S$) on $\mathfrak{X}_S$ is vertex transitive.*

Proof. Let $d_{\mathfrak{X}_p}$ be the distance function on $\mathfrak{X}_p$ under which adjacent vertices are distance one and d the distance on $\mathfrak{X}_S$ defined by summing the distances on components. If Γ_S does not act transitively on $\mathfrak{X}_S$, then there is a vertex v with minimal positive distance from v_0 that is not in the orbit $\Gamma_S \cdot v_0$. We claim that $d(v_0, v) = 1$. If not, then there is a vertex v' with $d(v_0, v') < d(v_0, v)$ and $d(v', v) < d(v_0, v)$, since the $\mathfrak{X}_p$ are trees. However, then there is a $\sigma \in \Gamma_S$ such that $\sigma v_0 = v'$ and $d(v_0, \sigma^{-1} v) = d(v', v) < d(v_0, v)$, so there is a $\tau \in \Gamma_S$ with $\tau v_0 = \sigma^{-1} v$. This would give $\sigma\tau v_0 = v$, contradicting $v \notin \Gamma_S \cdot v_0$, so in fact $d(v_0, v) = 1$.

We conclude that $v = (v_p)_{p \in S}$ has the property that there is a unique $p \in S$ such that $v_p \neq v_{0,p}$. Consider the set $N(v_{0,p})$ of vertices in $\mathfrak{X}_p$ adjacent to $v_{0,p}$. To prove the theorem, it suffices to show that $N(v_{0,p}) = T(p) \cdot v_{0,p}$ for each $p \in S$ at which B splits, where $T(p) \subset \Gamma_S$ is the set of elements of $\mathcal{O}$ with reduced norm p. Indeed, this proves that $\overline{\Gamma}_S$ sends v_0 to any vertex of $\mathfrak{X}_S$ at distance one from v_0 which, by the previous paragraph and the fact that $T(p) \cdot v_{0,q} = v_{0,q}$ for $q \neq p$, implies that $\overline{\Gamma}_S$ must act transitively on the vertices of $\mathfrak{X}_S$.

It is easy to see that indeed $T(p) \cdot v_{0,p} \subseteq N(v_{0,p})$. If $\sigma, \tau \in T(p)$ with $\tau v_0 = \sigma v_0$, then $\tau^{-1}\sigma$ stabilizes v_0 and has reduced norm 1, so it lies in $\mathcal{O}^*$. Thus, to prove that $T(p) \cdot v_{0,p} = N(v_{0,p})$, it suffices to show that there are exactly $p + 1 = \#N(v_{0,p})$ cosets of $\mathcal{O}^*$ in $T(p)$, which follows immediately from our assumptions on $\mathcal{O}$. Indeed, there are then $p + 1$ ideals of index p^2 in $\mathcal{O}$ containing the ideal $p\mathcal{O}$. Each such ideal that is principal gives a $\mathcal{O}^*$-orbit of elements with reduced norm p. □

Remark 2.2. In fact, the proof shows something stronger, which we will need in Algorithms 2.6 and 2.7 below. For any element $\overline{g} \in \overline{\Gamma}_S$ mapping v_0 to $v' = \{v'_p\}_{p \in S}$ with $d_{\mathfrak{X}_p}(v_{0,p}, v'_p) \leq 1$ for each $p \in S$, there exists an element $x \in \mathcal{O}$ of reduced norm dividing $m_S := \prod_{p \in S} p$ such that $\bar{x} = \bar{g}$.

We now prove that Theorem 2.1 applies to Hamilton's quaternion algebra $\mathcal{H}$ over $\mathbb{Q}$. Two of the authors proved this as an application of the main

result of their joint paper [3]. For completeness we give an alternate proof of a more classical flavor that replaces [3] with an application of Jacobi's theorem on sums of four squares. See also [1].

Corollary 2.3. *Let $\mathcal{H}$ be Hamilton's rational quaternion algebra, $\mathcal{M} \subset \mathcal{H}$ the Hurwitz order, S be a finite set of primes, and Γ_S the associated S-unit group. Then Γ_S acts transitively on the vertices of $\mathfrak{X}_S$.*

Proof. It suffices to show that there are exactly $p+1 = \#N(v_{0,p})$ cosets of $\mathcal{M}^*$ in $T(p)$. This is a consequence of $\#\mathcal{M}^* = 24$ together with Jacobi's theorem on sums of four squares. More precisely, there are exactly $24(p+1)$ elements of odd prime reduced norm p in $\mathcal{M}$. To see this, note that the equation $(a/2)^2 + (b/2)^2 + (c/2)^2 + (d/2)^2 = p$ for $a, b, c, d \in \mathbb{Z}$ implies that they are either all even or all odd and thus

$$\frac{1}{2}(a + bI + cJ + dIJ) \in \mathcal{M}.$$

Now multiply by 4 and apply the even case of Jacobi's theorem. □

Applying Theorem 2.1, we obtain a fundamental domain

$$R_S = \prod_{p \in S} R_p \tag{2}$$

for the action of Γ_S on $\mathfrak{X}_S$, where

$$R_p = \left\{ (x_p)_{p \in S} \ : \ d_{\mathfrak{X}_p}(x_p, v_{0,p}) < \frac{2}{3} \text{ for all } p \right\}. \tag{3}$$

Here, by fundamental domain we mean an open set U with compact closure such that $\Gamma_S \cdot U = \mathfrak{X}_S$. The action of Γ_S on $\mathfrak{X}_S$ factors through $\overline{\Gamma}_S$, and R_S is also a fundamental domain for the action of $\overline{\Gamma}_S$. Furthermore, the stabilizer of v_0 in $\overline{\Gamma}_S$ is the image of $\mathcal{O}^*$ in $\overline{\Gamma}_S$, which is a finite subgroup. We can then find a presentation for $\overline{\Gamma}_S$ via the following theorem of Macbeath ([5], see also [8, §I.3]).

Theorem 2.4. *Let X be a path connected and simply connected topological space, G a group of homeomorphisms of X, and $U \subseteq X$ a path connected open set such that $GU = X$. Let*

$$\Sigma = \{ g \in G \ : \ U \cap gU \neq \emptyset \}$$

and let $F(\Sigma)$ be the free group on Σ with generators x_σ for $\sigma \in \Sigma$. Then the homomorphism $F(\Sigma) \to G$ given by sending x_σ to σ is surjective with

kernel equal to the normal subgroup of $F(\Sigma)$ generated by the words of the form $x_\sigma x_\tau x_{\sigma\tau}^{-1}$ for every pair $\sigma, \tau \in \Sigma$ such that

$$U \cap \sigma U \cap \sigma\tau U \neq \emptyset.$$

Remark 2.5. Note that for any σ, $\tau \in \Sigma$, we can always add the relation $x_\sigma x_\tau = x_{\sigma\tau}$ to our presentation for G, and thus instead of checking triple intersections we can check for triples satisfying the weaker condition that $\sigma\tau \in \Sigma$ for $\sigma, \tau \in \Sigma$, at the price of adding some redundant relations.

We then have the following algorithm. For simplicity, for the remainder of this section we consider S containing only primes that split B. Our arguments work without modification when S contains primes that ramify B, so we only make this assumption to simplify notation. Recall that $m_S = \prod_{p \in S} p$. In what follows, $\overline{X}$ denotes the image of a subset or element X of Γ_S in $\overline{\Gamma}_S$.

Algorithm 2.6.
Input: *A definite rational quaternion algebra B, an order $\mathcal{O}$ of B, and a finite set S of rational primes that split B such that, for every $p \in S$ at which B splits, the localization $\mathcal{O}_p$ of $\mathcal{O}$ at p is a maximal order of B_p and all left ideals of $\mathcal{O}$ of norm p are principal.*
Output: *A presentation for the projective S-unit group $\overline{\Gamma}_S$ with generators*

$$A = \left\{ a_{\overline{x}} \ : \ \overline{x} \in \overline{\mathcal{O}} \text{ for } x \in \mathcal{O} \text{ with } \mathrm{N}(x) \mid m_S \right\}$$

and relations

$$\mathcal{R} = \left\{ a_{\overline{\sigma}}\, a_{\overline{\tau}}\, a_{\overline{\nu}}{}^{-1} = 1 \ : \ (a_{\overline{\sigma}},\, a_{\overline{\tau}},\, a_{\overline{\nu}}) \in Y \right\},$$

where Y is the set of triples $(a_{\overline{\sigma}}, a_{\overline{\tau}}, a_{\overline{\nu}}) \in A^3$ such that $\overline{\sigma}\,\overline{\tau} = \overline{\nu}$.

Proof. We need to show that the map $a_{\overline{x}} \mapsto \overline{x}$ is an isomorphism between the abstract group with generators A and relations $\mathcal{R}$ and $\overline{\Gamma}_S$. By Theorem 2.4 and Remark 2.5, it suffices to show that elements $a_{\overline{x}}$ of A represent exactly those elements $\overline{x} \in \overline{\Gamma}_S$ such that $\overline{x} R_S \cap R_S \neq \emptyset$, where R_S is the fundamental domain for the action of $\overline{\Gamma}_S$ defined in (2). Indeed, this means precisely that our generators are the generators given by Theorem 2.4, and our relations are the relations given by Theorem 2.4 plus the possibly redundant relations considered in Remark 2.5.

If $a_{\overline{x}} \in A$ then for any $p \in S$, the associated element $x \in \mathcal{O}$ of reduced norm dividing m_S has reduced norm in $p^\epsilon \mathbb{Z}_p^*$ for $\epsilon \in \{0, 1\}$ and hence either

fixes $v_{0,p}$ (i.e., $\epsilon = 0$ and x stabilizes the standard lattice $\mathcal{L}_{0,p}$ defined in (1)) or maps $v_{0,p}$ to a neighbor in $\mathfrak{X}_p$ (i.e., $\epsilon = 1$ and x maps $\mathcal{L}_{0,p}$ to an index p sublattice). When $\epsilon = 1$, notice that $x^{-1}v_{0,p}$ is also a neighbor of $v_{0,p}$, and thus the midpoint of the edge between $v_{0,p}$ and $x^{-1}v_{0,p}$ maps under x to the midpoint of the edge between $v_{0,p}$ and $x\,v_{0,p}$. It follows that $\overline{x}R_p \cap R_p \neq \emptyset$ for each $p \in S$, with R_p as in (3). Thus $\overline{x}R_S \cap R_S \neq \emptyset$, and so $a_{\overline{x}}$ is one of the generators defined in Theorem 2.4.

Conversely, suppose that $\gamma \in \Gamma_S$ has the property that $\gamma R_S \cap R_S \neq \emptyset$, so Theorem 2.4 says there should be a generator in A associated with γ. It follows immediately from Remark 2.2 that there exists some $x \in \mathcal{O}$ such that $\mathrm{N}(x) \mid m_S$ and $\overline{x} = \overline{\gamma}$. Therefore, γ is associated with a generator $a_{\overline{x}} \in A$. Therefore A is exactly the generating set from Theorem 2.4, and we are done. □

We also have the following improved algorithm, which produces more efficient presentations.

Algorithm 2.7.
Input: *A definite rational quaternion algebra B, an order $\mathcal{O}$ of B, and a finite set S of rational primes that split B such that, for every $p \in S$ at which B splits, the localization $\mathcal{O}_p$ of $\mathcal{O}$ at p is a maximal order of B_p and all left ideals of $\mathcal{O}$ of norm p are principal.*
Output: *A presentation for the projective S-unit group $\overline{\Gamma}_S$ with generators A' and relations $\mathcal{R}'$.*

The generators are of the form

$$A' = A_0 \cup \bigcup_{p \in S} A_p,$$

where

$$A_0 = \{a_{\overline{x}} \ : \ \overline{x} \in \overline{\mathcal{O}}^*,\ \overline{x} \neq 1\},$$

and A_p consists of elements $a_{\overline{x}}$ for each vertex v in $N(v_{0,p})$, where we choose one $\overline{x} \in \overline{\mathcal{O}}$ such that $\overline{x}\,v_{0,p} = v$ for some $v \in N(v_{0,p})$ and $\overline{x}$ has a representative $x \in \mathcal{O}$ with $\mathrm{N}(x) = p$. Equivalently, A_p consists of exactly one element for each of the $p+1$ orbits of the right action of $\mathcal{O}^*$ on the set elements of $\mathcal{O}$ of reduced norm p.

The relations $\mathcal{R}'$ are all those of the following four types:

1. *$a_{\overline{\sigma}}a_{\overline{\tau}}a_{\overline{\nu}}{}^{-1} = 1$ when $a_{\overline{\sigma}}, a_{\overline{\tau}}, a_{\overline{\nu}} \in A_0$ such that $\overline{\sigma}\,\overline{\tau} = \overline{\nu}$;*
2. *$a_{\overline{\sigma}}a_{\overline{\tau}}a_{\overline{\nu}}{}^{-1} = 1$ when $a_{\overline{\sigma}}, a_{\overline{\tau}} \in A_p$ for some $p \in S$ and $a_{\overline{\nu}} \in A_0$ with $\overline{\sigma}\,\overline{\tau} = \overline{\nu}$;*

3. $a_{\overline{\sigma}}a_{\overline{\tau}}(a_{\overline{\nu}}a_{\overline{\alpha}}a_{\overline{\beta}})^{-1} = 1$ *when* $a_{\overline{\sigma}}, a_{\overline{\beta}} \in A_p$ *and* $a_{\overline{\tau}}, a_{\overline{\alpha}} \in A_q$ *with* $q < p$ *and* $a_{\overline{\nu}} \in A_0$ *all satisfy* $\overline{\sigma}\,\overline{\tau} = \overline{\nu}\,\overline{\alpha}\,\overline{\beta}$*;*

4. $a_{\overline{\nu}}a_{\overline{\sigma}}(a_{\overline{\tau}}a_{\overline{\mu}})^{-1} = 1$ *when* $a_{\overline{\sigma}}, a_{\overline{\tau}} \in A_p$ *and* $a_{\overline{\nu}}, a_{\overline{\mu}} \in A_0$ *with* $\overline{\nu}\,\overline{\sigma} = \overline{\tau}\,\overline{\mu}$*.*

Proof. We first show that, considered as elements of $\overline{\Gamma}_S$, the generators of Algorithm 2.6 can be obtained from these generators.

Let $z \in \mathcal{O}$ be an element of reduced norm dividing m_S. Then z maps $v_0 = (v_{0,p})_{p\in S}$ to a vertex

$$v = (v_p)_{p\in S} \in N(v_0) = \prod_{p\in S} N(v_{0,p}).$$

We claim there is an element $y = y_1 \cdots y_n \in \mathcal{O}$ with either $a_{\overline{y}_j} \in A_{p_j}$ $(p_1 < \cdots < p_n)$ or $y_j = 1$, such that y maps v to v_0. First, note that each y_i has reduced norm p_i, and hence fixes v_{0,p_j} for $j \neq i$, but will permute its neighbors in $\mathfrak{X}_{p_i}$. Therefore, we take $y_i \in \mathcal{O}$ to be 1 if $v_{p_i} = v_{0,p_i}$ or a representative in $\mathcal{O}$ of an element of A_{p_i} that sends $y_{i+1}\cdots y_n\, v_{p_i}$ to v_{0,p_i} otherwise. Then $y_i \cdots y_n$ maps v_{p_j} to v_{0,p_j} for each $1 \leq i \leq n$. The resulting element y then maps v to v_0, as claimed.

Then zy is in the stabilizer of v_0, so the image of zy in $\overline{\Gamma}_S$ lies in $\overline{\mathcal{O}}^*$. Therefore, there exists a unique $a_{\overline{x}} \in A_0 \sqcup \{1\}$ such that $\overline{z} = \overline{x}\,\overline{y}^{-1}$ in $\overline{\Gamma}_S$, where $x \in \mathcal{O}$ represents $\overline{x} \in \overline{\mathcal{O}}^*$. Since Algorithm 2.6 shows that the $\overline{z}$ with $z \in \mathcal{O}$ of reduced norm dividing m_S generate $\overline{\Gamma}_S$, it follows that the elements $\overline{x}$ for $a_{\overline{x}} \in A'$ also generate $\overline{\Gamma}_S$.

The map ψ from the group with generators A' and relations $\mathcal{R}'$ to $\overline{\Gamma}_S$ generated by $a_{\overline{x}} \mapsto \overline{x}$ is well defined since each element of $\mathcal{R}'$ comes from an identity in $\overline{\Gamma}_S$. Since we wrote any generator of $\overline{\Gamma}_S$ coming from A as a word in the $\psi(a_{\overline{x}})$ for $a_{\overline{x}} \in A'$, ψ is surjective. All that remains to be shown is that if w is a word in the generators A' such that $\psi(w)$ is the identity, we can use the relations in $\mathcal{R}'$ to reduce w to the identity.

We first claim that, for every $a_{\overline{\sigma}} \in A_p$ and $a_{\overline{\nu}} \in A_0$, there exist $a_{\overline{\tau}} \in A_p$ and $a_{\overline{\mu}} \in A_0$ such that $\overline{\nu}\,\overline{\sigma} = \overline{\tau}\,\overline{\mu}$. In other words, we can move a generator from A_p across a generator of type A_0 using relations in $\mathcal{R}'$. The associated elements $\overline{\nu}\,\overline{\sigma} \in \overline{\mathcal{O}}$ fix $v_{0,q}$ for $p \neq q$ and send $v_{0,p}$ to a vertex adjacent to $v_{0,p}$. Thus there is a unique $a_{\overline{\tau}} \in A_p$ such that

$$\overline{\nu}\,\overline{\sigma} \cdot v_{0,p} = \overline{\tau} \cdot v_{0,p}.$$

Then $\overline{\tau}^{-1}$ also fixes $v_{0,q}$ for $q \neq p$, so $\overline{\tau}^{-1}\overline{\nu}\,\overline{\sigma}$ fixes v_0. Therefore

$$\overline{\tau}^{-1}\overline{\nu}\,\overline{\sigma} = \overline{\mu}$$

for some $\overline{\mu} \in \overline{\mathcal{O}}^*$. This proves the claim.

Similarly, given $a_{\overline{\sigma}} \in A_p$ and $a_{\overline{\tau}}, \in A_q$ with $q < p$, we claim that there exist $a_{\overline{\beta}} \in A_p$, $a_{\overline{\alpha}} \in A_q$, and $a_{\overline{\nu}} \in A_0$ such that

$$\overline{\sigma}\,\overline{\tau} = \overline{\nu}\,\overline{\alpha}\,\overline{\beta}.$$

Indeed, $\overline{\sigma}\,\overline{\tau}$ fixes $v_{0,\ell}$ for $\ell \neq p, q$, and moves each of $v_{0,p}, v_{0,q}$ to a neighbor in its respective Bruhat–Tits tree. As in the proof of the previous claim, we can find $a_{\overline{\beta}} \in A_p$ and $a_{\overline{\alpha}} \in A_q$ so that

$$\overline{\alpha}^{-1}\overline{\beta}^{-1}\overline{\sigma}\,\overline{\tau} \cdot v_0 = v_0,$$

and is hence equal to some $\overline{\nu} \in \overline{\mathcal{O}}^*$, which proves the claim. Note that a similar statement also holds for inverses of our generators.

By the above, we can use relations of type (3) to move a generator from A_p or its inverse to the left across a generator from A_q ($p < q$), at the expense of possibly introducing a generator of type A_0 to the left and, of course, possibly changing which element of A_0 or A_p appears in the word. Similarly, relations of type (4) allow us to move a generator from A_0 or its inverse across a generator of type A_p for some $p \in S$, again possibly changing which element of A_0 and A_p appears. Applying these relations to consecutive positive or negative powers of generators appearing in the word, we can use the relations to assume that the word w is of the form

$$w = w_0 w_{p_1} \cdots w_{p_n}$$

where $S = \{p_1, \ldots, p_n\}$ ($p_1 < \cdots < p_n$) and w_r is a (possibly empty) word in the generators from A_r, $r \in S \cup \{0\}$.

Since $\psi(w)$ is the identity, $\psi(w_p)$ must send $v_{0,p}$ to $v_{0,p}$ for each $p \in S$, since no $\psi(w_q)$ for $q \neq p$ moves $v_{0,p}$. Relations of type (2) allow us to replace w_p with an element of A_0. Finally, using relations of type (1), we combine what remains into single generator corresponding to an element from A_0 that acts trivially on $\mathfrak{X}_S$ realized as an element of $\overline{\mathcal{O}}^*$, and which therefore is the identity in the group with generators A' and relations $\mathcal{R}'$. This completes the proof. □

It would be interesting to implement the results in [3] to present the S-units of any definite quaternion algebra over $\mathbb{Q}$, provided S is "large enough" as defined in [3]. Typically the action will not be vertex transitive, which we used to give particularly nice presentations, but ideas analogous to the above can still give an algorithm to compute explicit presentations.

3 Remarks on the congruence subgroup problem

In this section, we use our presentations to conduct some experiments related to the congruence subgroup problem for the S-units Γ_S of the Hurwitz order $\mathcal{M}$ of Hamilton's quaternions $\mathcal{H}$ over $\mathbb{Q}$. Our results do not confirm or disprove the conjecture in any new cases, but do give evidence for the conjecture. We begin by briefly describing this problem, which is open Γ_S when S contains at least two odd primes, i.e., when $\mathfrak{X}_S$ is a product of at least two trees. See [6] for more detailed surveys of the congruence subgroup problem.

A natural family of finite index subgroups of Γ_S arise from the *congruence subgroups*, which are defined as follows. Let I be a nonzero two-sided ideal of $\mathcal{M}_S$. The *congruence kernel of level* I, denoted $\Gamma_S(I)$, is subgroup of elements of Γ_S congruent to the identity modulo I.

We can also define the congruence kernels as follows. For odd $p \notin S$, embed $\mathcal{H}$ in $\mathrm{M}_2(\mathbb{Q}_p)$. Since $\mathcal{M}$ is a maximal order of $\mathcal{H}$, we can choose this embedding such that it induces an isomorphism of $\mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ with $\mathrm{M}_2(\mathbb{Z}_p)$. It follows that Γ_S embeds as a subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$, from which we obtain a map

$$\rho_{p^r} : \Gamma_S \to \mathrm{GL}_2(\mathbb{Z}_p/p^r\mathbb{Z}_p).$$

The kernel of ρ_{p^r} is precisely $\Gamma_S(I)$ for $I = \mathcal{P}^r$, where $\mathcal{P}$ is the prime of $\mathcal{M}_S$ with residue field $\mathbb{F}_p$, and we can extend this to arbitrary I via the Chinese Remainder Theorem.

This leads to the following important question.

Congruence Subgroup Problem. *For every finite index subgroup* Λ *of* Γ_S*, does there exists a nonzero two-sided ideal* I *of* $\mathcal{M}_S$ *such that* $\Gamma_S(I) < \Lambda$*?*

If the answer to the above question is yes, then Γ_S is said to have the *congruence subgroup property* (CSP). Otherwise, we say that the CSP fails. When $S = \emptyset$, $\Gamma_S = \mathcal{M}^*$ is finite and one can find a proper ideal I of $\mathcal{M}$ such that $\mathcal{M}^*(I) = \{1\}$. Therefore the trivial subgroup is a congruence kernel and $\mathcal{M}^*$ has the congruence subgroup property.

It is well known that Γ_S does not have the CSP when S contains exactly one odd prime. One way to see this is to observe that Γ_S acts discretely and cocompactly on the tree $\mathfrak{X}_S$ in this case. It is shown in [8, Part I] that Γ_S therefore contains a nonabelian free subgroup F of finite index. Let K be the kernel of a homomorphism of F onto the alternating group A_6. We claim that K is a finite index subgroup of Γ_S that does not contain a congruence

kernel. Indeed, one can show that A_6 is not isomorphic to a subquotient of

$$\prod_{q \in \mathcal{Q}} \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) \tag{4}$$

for any finite set $\mathcal{Q}$ of prime powers, and since every group $\Gamma_S/\Gamma_S(I)$ is a subgroup of some group of the form (4), so K cannot contain any $\Gamma_S(I)$.

Remark 3.1. Instead of A_6, we can choose one of the infinitely many finite groups that is not a quotient of a subgroup of some $\prod \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$.

Remarkably, the above basically sums up all our knowledge about the congruence subgroup problem for S-unit groups of $\mathcal{H}$. There is a similar lack of knowledge for S-unit groups of arbitrary quaternion division algebras over number fields. The following exhausts the previous results that we know.

Theorem 3.2. *Let k be a number field and B a k-quaternion algebra. For a maximal order $\mathcal{M}$ and a finite set of nonarchimedean places S of k, let Γ_S be the associated S-unit group.*

1. *If Γ_S is finite, then it has the congruence subgroup property.*
2. *(Serre [7]) If $B \cong \mathrm{M}_2(k)$, then Γ_S has the congruence subgroup property if and only if the ring of S-integers of k contains a unit of infinite order.*
3. *(Lubotzky [4]) If B is a division algebra and Γ_S is a lattice in $\mathrm{GL}_2(K)$ for any local field K of characteristic zero, then Γ_S does not have the congruence subgroup property.*

For B and Γ_S as in Theorem 3.2, we know of no further results about the congruence subgroup problem. In particular, as far as we know, for $\mathcal{H}$ the congruence subgroup problem for Γ_S is open in all cases except when S contains at most one odd prime. It is sometimes called Serre's Conjecture that when S contains at least two odd primes, Γ_S and $\overline{\Gamma}_S$ should have the congruence subgroup property. The remainder of this section collects some data related to this important open question.

Using MAGMA [2], we computed finite index subgroups of $\overline{\Gamma}_S$ for various S containing at least two primes. All of our observations support the congruence subgroup property holding when S contains at least two odd primes. We considered all finite quotients of $\overline{\Gamma}_S$ of order at most n for some small S. In Table 1 we tabulate all the groups which occur in composition series for such quotients for the S and n indicated.

S	n	$\mathbb{Z}/m\mathbb{Z}$	$\mathrm{PSL}_2(\mathbb{F}_p)$
$\{3,5\}$	30,000	$2,3$	$7,11,13,17,19,23,29,31$
$\{5,11\}$	20,000	$2,3$	$7,13,17,19,23$
$\{37,43\}$	15,000	$2,3,5$	$5,7,11,13,17,19,23$
$\{3,5,7\}$	20,000	$2,3$	$11,13,17,19,23$
$\{3,7,11\}$	20,000	$2,3,5$	$5,13,17,19,23$
$\{7,11,13\}$	15,000	$2,3,5$	$5,17,19,23$
$\{11,13,17,19\}$	10,000	$2,3$	$5,7$
$\{3,5,7,11,13\}$	10,000	$2,3$	$17,19$

Table 1: Groups appearing in the composition series for finite quotients of $\overline{\Gamma}_S$ of order $\leq n$.

We now briefly describe why our experiments are consistent with the congruence subgroup property, even though many quotients are not exactly of the form $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$. Cyclic composition factors arise from either the congruence subgroups of the unique maximal order in $\mathcal{M}_2$, quotients of the binary tetrahedral group, or the soluble part of $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Finally, note in particular that there are no homomorphisms onto A_6.

4 Presentations

We now tabulate presentations for $\overline{\Gamma}_S$ for several small values of S. Since we are considering the projective units,we give an integral representative for each generator, that is, an element of $\mathbb{Z}[1, I, J, IJ]$. To our knowledge, these are the first known presentations of S-arithmetic lattices in a semisimple Lie group where S contains at least two places at which the associated algebraic group is isotropic (i.e., not compact). Unpublished work of the late Fritz Grunewald presented some groups Γ^1_S, the subgroup of elements of reduced norm 1, for many small S contained in this paper, but unfortunately we were not able to obtain a copy of this work.

S = {3, 5}

Generators:

$$a = -1 + I - J - 3IJ$$
$$b = -9 - 7I - J + 7IJ$$

Relators:

$$
\begin{aligned}
r_1 =& (b^{-1}a^{-1}ba^{-1})^3 \\
r_2 =& (b^{-1}a^{-2}ba^{-1}b^{-1}a^{-1})^2 \\
r_3 =& (a^{-1}b^{-1}a^{-1}b^{-1}a^{-1}ba^{-1})^2 \\
r_4 =& b^{-1}abab^{-1}a^{-1}b^2ab^{-1}aba^2b^{-1}abab^{-1}a^2ba^2b^{-1}a^{-1}ba^{-2}b^{-1}a^{-2} \\
r_5 =& (ba^2b^{-1}aba^{-1}b)^2 \\
r_6 =& b^{-1}a^3ba^2b^{-1}ab^{-1}a^{-2}ba^{-1}b^{-1}a \\
r_7 =& b^{-2}a^{-1}ba^{-1}b^{-1}aba^2b^{-2}a^{-2}ba^{-1} \\
r_8 =& ab^{-1}a^2ba^{-1}b^{-1}a^{-2}ba^{-2}b^{-1}aba
\end{aligned}
$$

S = {3, 7}

Generators:

$$
\begin{aligned}
a =& -1 + I - J - 3IJ \\
b =& -1 - I - J - 5IJ
\end{aligned}
$$

Relators:

$$
\begin{aligned}
r_1 =& baba^{-2}bab^{-1}a^{-1}b^{-1}a^2b^{-1}a^{-1} \\
r_2 =& a^3ba^{-2}baba^2b^{-1}a^{-1}b^{-3}a^{-1}b^{-1} \\
r_3 =& bab^{-1}a^{-1}b^{-1}a^{-1}bab^2ab^2a^{-2}bab \\
r_4 =& (a^2b^{-1}a^{-1}b^{-2}a^{-1}b^{-1}a)^2 \\
r_5 =& ab^3ab^3aba^{-2}ba^3ba^{-2}b \\
r_6 =& b^{-2}ab^2aba^{-2}b^3aba^{-2}b^2a^2b^{-1}a^{-1}b^{-2}a^{-1}b^{-2}a^{-1}
\end{aligned}
$$

S = {3, 11}

Generators:

$$
\begin{aligned}
a =& 1 + I - J - IJ \\
b =& -1 - I - J - 3IJ \\
c =& -1 + I - 3IJ
\end{aligned}
$$

Relators:

$$\begin{aligned}
r_1 =& a^3 \\
r_2 =& (b^{-1}ca^{-1})^2 \\
r_3 =& (b, a^{-1})^2 \\
r_4 =& (c^{-1}ba^{-1}b)^2 \\
r_5 =& ba^{-1}b^-2ac^{-1}ab^{-1}c^{-1} \\
r_6 =& c^{-1}ab^{-1}c^{-1}acb^{-1}a^{-1}c^{-1} \\
r_7 =& (b^2a^{-1}b^{-1}a^{-1})^2 \\
r_8 =& (bab^{-1}a^{-1}c^{-1})^2
\end{aligned}$$

S = {5, 7}

Generators:

$$\begin{aligned}
a =& 1 - I + J - IJ \\
b =& - J - 2IJ \\
c =& - 1 + I + J - 5IJ
\end{aligned}$$

Relators:

$$\begin{aligned}
r_1 =& b^2 \\
r_2 =& a^3 \\
r_3 =& (c^{-1}ab)^2 \\
r_4 =& (a, c^{-1})^2 \\
r_5 =& (bca^{-1}c^{-1}a)^2 \\
r_6 =& (ca^{-1}c^{-1}a^{-1})^3 \\
r_7 =& cac^{-1}abcac^{-1}a^{-1}c^{-1}a^{-1}baca \\
r_8 =& c^{-1}a^{-1}bac^2ac^{-1}a^{-1}bacac^{-1}a
\end{aligned}$$

S = {3, 5, 7}

Generators:

$$\begin{aligned}
a =& 1 + I - J - IJ \\
b =& - 1 - I - J - 3IJ \\
c =& - I - 2IJ \\
d =& - 1 - I - J - 5IJ
\end{aligned}$$

Relators:

$$
\begin{aligned}
r_1 =& c^2 \\
r_2 =& a^3 \\
r_3 =& b^{-1}dad^{-1}ba^{-1} \\
r_4 =& bdcd^{-1}b^{-1}c \\
r_5 =& ca^{-1}d^{-1}cad \\
r_6 =& (d^{-1},a)^2 \\
r_7 =& (dba^{-1}d)^2 \\
r_8 =& (ca^{-1}b^2)^2 \\
r_9 =& (daba^{-1})^2 \\
r_{10} =& b^{-1}dcad^{-1}b^{-1}aca^{-1} \\
r_{11} =& ca^{-1}b^{-1}a^{-1}cda^{-1}d^{-1}b^{-1}a \\
r_{12} =& badad^{-1}ab^2ab^{-1}a \\
r_{13} =& d^{-1}b^{-1}a^{-1}bd^{-1}b^2adad^{-1} \\
r_{14} =& (a^{-1}da^{-1}d^{-1})^3 \\
r_{15} =& d^2ad^{-1}abd^{-1}a^{-1}da^{-1}d^{-1}b^{-1} \\
r_{16} =& d^{-1}a^{-1}b^{-1}acb^{-1}ad^{-1}aca^{-1}da^{-1}d^{-1} \\
r_{17} =& cda^{-1}d^{-1}a^{-1}d^{-1}a^{-1}b^{-1}acb^{-1}d^{-1}adad^{-1} \\
r_{18} =& (da^{-1}da^{-1}d^{-1}a^{-1}ca^{-1})^2
\end{aligned}
$$

S = {3, 5, 11}

Generators:

$$
\begin{aligned}
a =& -1 - I - J - 3IJ \\
b =& -1 - 2IJ \\
c =& -1 + J - 3IJ
\end{aligned}
$$

Relators:

$$
\begin{aligned}
r_1 &= b^2cba^{-1}c^{-2}b^{-1}ac^{-1} \\
r_2 &= (b^{-1}c^{-1}b^{-1}ac^{-1}a^{-1})^2 \\
r_3 &= bcbaba^{-1}b^{-1}c^{-1}b^{-1}ac^{-1}b^{-1}ca^{-1} \\
r_4 &= bac^{-1}b^{-1}ac^{-1}a^2b^{-1}c^{-1}b^{-1}ac^{-1}a \\
r_5 &= b^{-2}a^{-1}b^{-1}c^{-1}b^{-1}c^{-1}b^{-1}ac^{-1}aba^{-1}b^{-1}c^{-1}b^{-1} \\
r_6 &= bac^{-1}b^{-1}ac^{-1}ab^{-1}ca^{-1}ca^{-1}bca^{-1}c^{-1} \\
r_7 &= ca^{-1}bcb^{-1}a^{-1}b^{-1}cb^{-1}c^{-1}b^{-1}ac^{-1}abc \\
r_8 &= cb^2ac^{-1}b^{-1}ac^{-1}aca^{-1}bcba^{-1}ca^{-1}b \\
r_9 &= a^{-1}c^{-1}a^{-1}ca^{-1}bcb^{-1}ac^{-1}bab^{-1}c^{-1}b^{-2}ac \\
r_{10} &= c^2a^{-1}bcba^{-2}c^{-2}b^{-1}a^2b^{-1}c^{-1}b^{-1}ab \\
r_{11} &= c^{-1}a^{-1}b^2cba^{-1}b^{-1}a^{-1}b^{-1}ab^2ac^{-1}b^{-1}ac^{-1} \\
r_{12} &= bcac^{-1}b^{-1}ac^{-1}ac^{-2}b^{-1}a^{-1}ca^{-1}bca^{-1}c \\
r_{13} &= (b^2ca^{-1}bcb^2a)^2 \\
r_{14} &= a^{-2}ca^{-2}ca^{-1}bca^{-1}ca^{-2}babc^{-1}b^{-1}ac^{-1} \\
r_{15} &= bab^2ac^{-1}b^{-2}ab^{-1}a^{-1}b^{-2}a^{-3}b^{-1}c^{-1}b^{-1}a \\
r_{16} &= acbcba^{-1}c^{-1}b^{-1}c^{-1}b^{-1}ac^{-1}bcbab^{-1}a^{-1}b^{-2}a^{-1}b^{-1} \\
r_{17} &= bab^2abac^{-1}ababc^{-1}b^{-1}ac^{-1}ba^{-1}bcba \\
r_{18} &= b^2ca^{-1}bca^{-1}cba^{-1}c^{-1}a^{-1}ca^{-1}bcba^{-1}ba^{-1}ba \\
r_{19} &= b^{-2}c^{-1}b^{-1}ac^{-1}ab^{-1}ab^{-1}a^{-1}b^{-2}a^{-1}bcb^{-1}a^{-1}ca^{-1}b^{-1}a \\
r_{20} &= (bac^{-1}a^{-1}ca^{-1}bcb^2a)^2 \\
r_{21} &= (c^{-1}a^{-2}ca^{-1}bcbc^{-1}b^{-1}ac^{-1}a^{-1})^2 \\
r_{22} &= a^{-1}bcbac^{-1}b^{-1}ac^{-1}a^3ca^{-1}bcb^{-1}a^{-1} \\
&\quad b^{-1}ca^{-1}bca^{-1}b^{-1}cb^{-2}c^{-1}b^{-1}ac^{-1}b^{-2}a^{-1}cbc
\end{aligned}
$$

References

[1] S. Adian, F. Grunewald, I. Lysionok, and J. Mennicke, On embeddings of $\mathrm{SL}(2,\mathbb{Z})$ into quaternion groups, *Math. Z.* 238(2):389–399, 2001.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] T. Chinburg and M. Stover. Small generators for S-unit groups of division algebras. Submitted.

[4] A. Lubotzky. Free quotients and the congruence kernel of SL_2. *J. Algebra*, 77(2):411–418, 1982.

[5] A. M. Macbeath. Groups of homeomorphisms of a simply connected space. *Ann. of Math. (2)*, 79:473–488, 1964.

[6] M. S. Raghunathan. The congruence subgroup problem. *Proc. Indian Acad. Sci. Math. Sci.*, 114(4):299–308, 2004.

[7] J.-P. Serre. Le problème des groupes de congruence pour SL2. *Ann. of Math. (2)*, 92:489–527, 1970.

[8] J.-P. Serre. *Trees*. Springer Monographs in Mathematics. Springer-Verlag, 2003.

[9] W. A. Stein et al. *Sage Mathematics Software (Version 5.12)*. The Sage Development Team. `http://www.sagemath.org`.

[10] M.-F. Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.