Small generators for S-unit groups of division algebras

Ted Chinburg and Matthew Stover

To H. W. Lenstra, Jr.

ABSTRACT. Let k be a number field, suppose that B is a central simple division algebra over k, and choose any maximal order $\mathcal{D}$ of B. The object of this paper is to show that the group $\mathcal{D}_S^*$ of S-units of B is generated by elements of small height once S contains an explicit finite set of places of k. This generalizes a theorem of H. W. Lenstra, Jr., who proved such a result when $B = k$. Our height bound is an explicit function of the number field and the discriminant of a maximal order in B used to define its S-units.

CONTENTS

1. Introduction

Let k be a number field, suppose that B is a central simple division algebra over k, and choose any maximal order $\mathcal{D}$ of B. The object of this paper is to show that the group $\mathcal{D}_S^*$ of S-units of k is generated by elements of small height once S contains an explicit finite set of places of k.

A result of this kind was shown by Lenstra in [7] when B is k itself. In this case, G is the multiplicative group $\mathbb{G}_m$ and the notion of height is the classical one. Lenstra showed that once S is sufficiently large, the group $\mathbb{G}_m(O_{k,S}) = O_{k,S}^*$ is generated by elements whose log heights are bounded by

$$\frac{1}{2} \log |d_{k/\mathbb{Q}}| + \log m_S + r_2(k) \log(2/\pi),$$

where d_k is the discriminant of k, m_S is the maximal norm of a finite place in S, and $r_2(k)$ is the number of complex places of k. One version of our results is the following.

Theorem 1.1. *Suppose B is a central simple division algebra of dimension d^2 over a number field k, $n = [k : \mathbb{Q}]$, and s is the number of real places of k over which B ramifies. Then there is a maximal order $\mathcal{D}$ of B with discriminant $d_\mathcal{D}$ and functions $f_1(n,d)$ and $f_2(n,d)$ of integer variables n and d for which the following is true. Define*

$$e = \frac{2n}{d(2n - s)}.$$

Suppose that S is a finite set of places of k containing all the archimedean places and that S contains all finite places v such that

$$\text{Norm}(v) \leq f_1(n,d)\, d_\mathcal{D}^e.$$

Let m_{S_f} be the maximum norm of a finite place in S. Then $e \leq 1$ and the group Γ_S of S-units in B with respect to the order $\mathcal{D}$ is generated by the finite set of elements of height bounded above by

$$f_2(n,d)\, m_{S_f}\, d_\mathcal{D}^e.$$

See the remarks at the end of §5.6 for explicit expressions for $f_1(n,d)$ and $f_2(n,d)$. In many cases (e.g., when B is a number field) we have

$$(1) \qquad f_1(n,d) = d^{nd} \left(\frac{2}{\pi}\right)^{\frac{ndr_2}{n-s/2}} \left(\frac{2\sqrt{2}}{\pi}\right)^{\frac{nds}{2n-s}}$$

$$(2) \qquad f_2(n,d) = d^{nd+n+s} \left((d-1)!\right)^{n-s} 2^{s\frac{d^2-2d-4}{2}} \left(\frac{2}{\pi}\right)^{\frac{ndr_2}{n-s/2}} \left(\frac{2\sqrt{2}}{\pi}\right)^{\frac{nds}{2n-s}}$$

where r_2 is the number of complex places of k and all other notation is from the statement of Theorem 1.1. Thus, when B is a number field this exactly reproduces Lenstra's bound.

When S is empty, even for a number field k one does not expect to be able to generate the unit group O_k^* by elements whose log heights are bounded by a polynomial in $\log |d_{k/\mathbb{Q}}|$. For example, the Brauer–Siegel Theorem implies that if k is real quadratic of class number 1, then the log height of a generator of O_k^* is greater than $c_\epsilon d_{k/\mathbb{Q}}^{1/2-\epsilon}$ for all $\epsilon > 0$, where $c_\epsilon > 0$ depends only on ϵ. However, to our knowledge there is no unconditional proof, even in the case of real quadratic fields, that there cannot be an upper bound on the log heights of generators for O_k^* that is polynomial in $\log |d_{k/\mathbb{Q}}|$.

To develop our counterpart of Lenstra's results, we must first define an intrinsic notion of height for elements of B^*. The role of $|d_{k/\mathbb{Q}}|$ is played by the discriminant $d_{\mathcal{D}}$ of an O_k-order $\mathcal{D}$ in B that is used to define the S-integrality of points of G over k. The height bound we produce applies to all choices of $\mathcal{D}$ once S is sufficiently large. It implies, in particular, that there is a maximal order $\mathcal{D}$ in B such that when S is sufficiently large (in an explicitly defined sense), one can generate the points of G over $O_{k,S}$ by elements whose log heights are bounded by $\frac{1}{2}\log |\Delta_{k/\mathbb{Q}}| + \log m_S + \mu$ where μ depends only only the degree of B over $\mathbb{Q}$. See [8], [9], [3] and references therein for work on heights on quaternion algebras.

To show that our bounds remain quite effective outside the number field setting, in §6 we apply our results to Hamilton's quaternion algebra over $\mathbb{Q}$. The main result is the following.

Theorem 1.2. *Let B be Hamilton's quaternion algebra over $\mathbb{Q}$, that is, the rational quaternion algebra with basis $\{1, I, J, IJ\}$ such that $I^2 = J^2 = -1$ and $IJ = -JI$. Let $\mathcal{D}$ be the maximal order*

$$\mathbb{Z}\left[1, I, J, \frac{1 + I + J + IJ}{2}\right]$$

and $S = \{\infty, \ell_1, \ldots, \ell_h\}$ be a set of places containing the archimedean place ∞ and any set $\{\ell_i\}_{i=1}^h$ of distinct odd primes. Then the unit group $\mathcal{D}_S^*$ is generated by the finite set of elements with reduced norm contained in $\{1, \ell_1, \ldots, \ell_h\}$.

As in Lenstra's case, Theorem 1.1 leads to an algorithm for finding generators for $O_{k,S}^*$. After embedding B into a real vector space, the algorithm is reduced to the classical problem of enumerating lattice points of bounded norm. That an algorithm exists to generate S-integral points of an algebraic group over a number field, with no assumptions on S, was known by work of Grunewald–Segal [5], [6]. Unlike their algorithm, ours is primitive recursive, which answers a question raised in [6].

Lenstra went on to show that his algorithm, together with linear algebra, can be used to give a deterministic algorithm for finding generators for

the unit group O_k^* with running-time $O_\epsilon(|d_{k/\mathbb{Q}}|^{3/4+\epsilon})$. The output of the algorithm consists of the digits of a set of generators. Answering a question raised by Lenstra, Schoof recently announced an improvement of this run-time to $O_\epsilon(|d_{k/\mathbb{Q}}|^{1/2+\epsilon})$. By the discussion of the Brauer–Siegel theorem above, one expects the length of the output may be on the order of $|d_{k/\mathbb{Q}}|^{1/2-\epsilon}$ in some cases, but the input to the problem, namely enough information to specify k, will in general be much shorter. For instance, a real quadratic field k can be specified by giving its discriminant $d_{k/\mathbb{Q}}$, and the number of bits necessary to specify $d_{k/\mathbb{Q}}$ is proportional to $\log |d_{k/\mathbb{Q}}|$.

Lenstra's algorithm for finding generators for O_k^* makes essential use of the fact that $O_{k,S}^*$ is abelian, and this is not the case when B is noncommutative and $\mathcal{D}_S^*$ is infinite. Consequently, we do not know a counterpart of this algorithm for producing generators in the general case.

We also note that there is a spectral approach to finding small generators for groups acting on symmetric spaces. For example, if V is a compact quotient of a rank one symmetric space other than hyperbolic 2- or 3-space, Burger and Schroeder [1] showed that one can bound the diameter of V from above in terms of its volume and $\lambda_1(V)\mathrm{diam}(V)$ in terms of $\log \mathrm{vol}(V)$. One can use this to bound the length (in the Riemannian metric on V) of a generating set. As noted in [1], these results fail for hyperbolic 2- and 3-space, though Peter Shalen informed us that one could prove an analogous theorem for arithmetic Fuchsian and Kleinian groups assuming Lehmer's conjecture. However, the problem we solve in this paper is of a different kind, even where a result like that of [1] holds. Our methods find explicit matrix generators with small entries, and it is not at all clear that generators that are short in an associated Riemannian metric have representatives in GL_n with small entries. It would be interesting to see if spectral methods for S-arithmetic subgroups of reductive groups could produce generators that have small height.

The main tool for producing small generators for $O_{k,S}^*$ once S is sufficiently large is Minkowski's lattice point theorem. This determines elements of B^* which can be shown to be S-integral by careful consideration of the constants required to apply Minkowski's theorem. In particular, the assumption that B is a division algebra is crucial, and it would be interesting to extend our results to unit groups of arbitrary central simple algebras. The reason we cannot work with a general central simple algebra is because Minkowski's lattice point theorem returns a nonzero element of the algebra B. We prove that it is S-integral. However, it might not be invertible in B if B is not a division algebra. Given that $\mathrm{SL}_n(\mathbb{Z})$ is generated by elementary matrices, which certainly have small height, we expect such a result to hold. It appears to us that it is a deep problem to extend such height results to generators for the S-integral points of more general linear algebraic groups over number fields.

2. Notation and definitions

Let k be a number field with ring of integers O_k and $[k : \mathbb{Q}] = n$. We denote by V_∞ (resp. V_f) the set of archimedean (resp. finite) places of k. Let B be a division algebra over k with degree d and let $\mathcal{D} \subset B$ be an O_k-order in B. The multiplicative group of units in a ring R will be denoted R^*. For each place v of k and any k-algebra or O_k-module A, let A_v denote the associated completion at v.

Define a norm on B_v^* by

$$\text{(3)} \qquad \text{Norm}_v(x_v) = \text{Norm}_{k_v/\mathbb{Q}_{p(v)}}(\det(x_v \curvearrowright B_v)),$$

where $p(v)$ is the place of $\mathbb{Q}$ under v and $x_v \curvearrowright B_v$ is the k_v-linear endo-morphism of B_v induced by left x_v-multiplication. If $\det_v : B_v \to k_v$ is the reduced norm, then

$$\text{(4)} \qquad \det(x_v \curvearrowright B_v) = \det_v(x_v)^d.$$

The idele group $J(B)$ is the restricted direct product $\prod_v' B_v^*$ of the B_v^* with respect to the groups $\mathcal{D}_v^*$. For $x = \prod_v x_v \in J(B)$, define

$$\text{(5)} \qquad \text{Norm}_\infty(x) = \prod_{v \in V_\infty} \text{Norm}_v(x_v)$$

$$\text{(6)} \qquad \text{Norm}_f(x) = \prod_{v \in V_f} \text{Norm}_v(x_v).$$

We view these norms as elements of the idele group $J(\mathbb{Q})$ of $\mathbb{Q}$ in the natural way. Let $|\,\,| : J(\mathbb{Q}) \to \mathbb{R}_{>0}$ be the usual norm. By the product formula,

$$\text{(7)} \qquad |\text{Norm}_\infty(x)| = |\text{Norm}_f(x)|^{-1}$$

for all $x \in B^*$.

Let S be a finite set of places of k containing V_∞. Set $S_f = S \smallsetminus V_\infty$, and consider the groups

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

$$B_{S_f}^* = \prod_{v \in S_f} B_v^* \subset B_f^* = \prod_{v \in V_f}{}' B_v^*$$

and the product

$$\text{(8)} \qquad B_S^* = \prod_{v \in S} B_v^* = B_\mathbb{R}^* \times B_{S_f}^* \subset J(B) = B_\mathbb{R}^* \times B_f^*.$$

Let G_S be the subgroup of B_S^* that satisfies the product formula, so

$$\text{(9)} \qquad G_S = \left\{ (x, \beta) \in B_S^* \,\,:\,\, |\text{Norm}_\infty(x)| = |\text{Norm}_f(\beta)|^{-1} \right\}.$$

If $O_{k,S}$ denotes the S-integers of k, i.e., those elements of k which lie in $O_{k,v}$ for all $v \notin S$, then the S-order of B associated with $\mathcal{D}$ is

$$\text{(10)} \qquad \mathcal{D}_S = O_{k,S} \otimes_{O_k} \mathcal{D}.$$

The group of invertible elements of $\mathcal{D}_S$ will be denoted Γ_S and is called the group of S-*units* of $\mathcal{D}$.

We define a topology on G_S by its natural embedding into B_S^*. The image of Γ_S in G_S under the diagonal embedding is a discrete subgroup. We have diagonal embeddings $\Gamma_S \to B_S^*$ and $\Gamma_S \to \prod_{v \notin S} \mathcal{D}_v^*$, and the product of these embeddings is the natural diagonal embedding of Γ_S into $J(B)$.

For any element

$$\alpha = \prod_{v \in V_f} \alpha_v \in B_f^*,$$

there is a right-$\mathcal{D}$-module

$$(11) \qquad \alpha\mathcal{D} = B \cap \left(\prod_{v \in V_f} \alpha_v \mathcal{D}_v \right),$$

where B is diagonally embedded in B_f. For $\alpha \in \mathcal{D}$, the index of $\alpha\mathcal{D}$ in $\mathcal{D}$ equals $|\mathrm{Norm}_f(\alpha)|^{-1}$. We also have the left-$\mathcal{D}$-module

$$(12) \qquad \mathcal{D}\alpha^{-1} = \{x \in B \ : \ x(\alpha\mathcal{D}) \subseteq \mathcal{D}\}.$$

3. Absolute values and heights

In this section we define absolute values on the completions B_v of B. These will be used to define our notion of height for elements of B^*. We point the reader to [8], [9], [3] and references therein for earlier work on heights for quaternion algebras over number fields.

For each place v of k there is a division algebra A_v over k_v such that $B_v = k_v \otimes_k B$ is isomorphic to a matrix algebra $\mathrm{M}_{m(v)}(A_v)$. The dimension of A_v over k_v is $d(v)^2$ for some integer $d(v)$ such that $d(v)m(v) = d = \sqrt{\dim_k B}$. Note that A_v and B_v have center isomorphic to k_v.

For finite v let O_v be the ring of integers of k_v. We fix isomorphisms $\rho_v : B_v \to \mathrm{M}_{m(v)}(A_v)$ such that for almost all finite v, $A_v = k_v$ and $\rho_v(\mathcal{D}_v) = \mathrm{M}_{m(v)}(O_v)$. Let $\mathrm{N}_v : A_v \to k_v$ be the reduced norm. Then $\mathrm{N}_v(r) = r^{d(v)}$ for any $r \in k_v \subseteq A_v$.

For all places v of k, let $|\ |_v$ be the usual normalized absolute value on k_v. We extend $|\ |_v$ to an absolute value on A_v by $|\alpha|_v = |\mathrm{N}_v(\alpha)|_v^{1/d(v)}$ for $\alpha \in A_v$. This absolute value is clearly multiplicative and restricts to the usual absolute value on the center k_v of A_v.

Suppose v is nonarchimedean. There is a unique maximal order U_v in A_v, namely the set of $\alpha \in A_v$ such that $|\alpha|_v \leq 1$. When $A_v \neq k_v$, U_v is a noncommutative local ring, and it is O_v when $A_v = k_v$. The unique maximal two-sided ideal of U_v is the set P_v of $\alpha \in A_v$ for which $|\alpha|_v < 1$. There is an element λ_v of P_v such that $P_v = U_v\lambda_v = \lambda_v U_v$; such λ_v are called prime elements by Weil in [12, Def. 3, Chap. I.4]. By [12, Prop. 5, Chap. I.4], $\mathrm{N}_v(\lambda_v)$ is a uniformizer in k_v. Thus $|\lambda_v|_v = |\mathrm{N}_v(\lambda_v)|_v^{1/d(v)} = (\#k(v))^{-1/d(v)}$ where $k(v)$ is the residue field of v and so the range of $|\ |_v$ on

A_v^* is $(\#k(v))^{1/d(v)})^{\mathbb{Z}}$. The set of $\alpha \in A_v^*$ such that $|\alpha|_v \leq (\#k(v))^{-t/d(v)}$ is exactly P_v^t. This implies that $|\alpha + \beta|_v \leq \max(|\alpha|_v, |\beta|_v)$ for every $\alpha, \beta \in A_v$.

We now prove a simple lemma.

Lemma 3.1. *With notation as above, suppose that v is archimedean. For all m-element subsets $\{\alpha_i\}_{i=1}^m \subset A_v$,*

$$(13) \qquad \left| \sum_{i=1}^m \alpha_i \right|_v \leq m^{[k_v:\mathbb{R}]-1} \sum_{i=1}^m |\alpha_i|_v.$$

Proof. If v is complex, then $A_v = k_v \cong \mathbb{C}$ and $|\ |_v$ is the square of the usual Euclidean absolute value. The result reduces to the Cauchy–Schwarz inequality. If v is real and $A_v = k_v \cong \mathbb{R}$, the lemma is again clear.

The final case is when v is real and A_v is Hamilton's quaternions $\mathbb{H} = \mathbb{R} + \mathbb{R}I + \mathbb{R}J + \mathbb{R}IJ$ where $I^2 = J^2 = -1$ and $IJ = -JI$. Here,

$$|a + bI + cJ + dIJ|_v = (a^2 + b^2 + c^2 + d^2)^{1/2}.$$

We can view this as the Euclidean length in $\mathbb{R}^4$ of the vector (a, b, c, d). It is clear from the triangle inequality that the optimal constant in this case is again 1. This proves the lemma. $\qquad \square$

Recall that for each place v of k we fixed an isomorphism

$$\rho_v : B_v \to \mathrm{M}_{m(v)}(A_v).$$

For each v and each $\gamma \in B_v^*$, let $\gamma^{i,j}(v)$ denote the (i,j)-component of the $m(v) \times m(v)$ matrix $\rho_v(\gamma) \in \mathrm{GL}_{m(v)}(A_v)$. Define $|\gamma|_v = \max_{i,j} |\gamma^{i,j}(v)|_v$. Embed B into $B_v = k_v \otimes_k B$ in the natural way. Then the *height* of $\gamma \in B^*$ is defined by

$$(14) \qquad \mathrm{H}(\gamma) = \prod_{v \in V} \max\{1, |\gamma|_v^{d(v)}\},$$

where the product is over the set $V = V_\infty \cup V_f$ of all places of k. From the definition of $|\ |_v$ we see that

$$(15) \qquad \mathrm{H}(\gamma) = \prod_{v \in V} \max \left\{ 1, \max_{i,j} |\mathrm{N}_v(\gamma^{i,j}(v))|_v \right\}.$$

For any S and any positive real number x, the set

$$(16) \qquad \mathrm{BH}_S(x) = \{\gamma \in \Gamma_S \ : \ \mathrm{H}(\gamma) \leq x\}$$

of S-units of $\mathcal{D}$ with height bounded by x is finite. Indeed, bounding the nonarchimedean height bounds the denominator of each matrix entry under the image of every ρ_v, so the set of $\gamma \in \Gamma_S$ with bounded height is contained in a lattice in $B_\mathbb{R}$. Bounding the archimedean height immediately implies finiteness.

We end this section by proving some inequalities we will need later concerning the behavior of absolute values on taking products and inverses of elements of B_v.

Lemma 3.2. *Suppose v is a finite place of k and fix an isomorphism*

$$\rho_v : B_v \to \mathrm{M}_{m(v)}(A_v).$$

Let $\det_v : B_v \to k_v$ be the reduced norm. For $y, y' \in B_v$:

1. $|yy'|_v \leq |y|_v\, |y'|_v.$
2. *If y is invertible, then $|\det_v(y)|_v\, |y^{-1}|_v^{d(v)} \leq |y|_v^{d(v)(m(v)-1)}.$*

Proof. Recall that

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

where

$$\rho_v(y) = (y^{i,j}(v))_{i,j} \in \mathrm{M}_{m(v)}(A_v).$$

Here $|q|_v = |\mathrm{N}_v(q)|_v^{1/d(v)}$ when $q \in A_v$, $\mathrm{N}_v : A_v \to k_v$ is the reduced norm and $\dim_{k_v}(A_v) = d(v)^2$. We noted earlier that $|qq'|_v = |q|_v|q'|_v$ and $|q + q'|_v \leq \max\{|q|_v, |q'|_v\}$ for $q, q \in A_v$, so statement *1.* of the lemma is clear by the usual matrix multiplication formula.

Let λ_v be a prime element of the unique maximal O_v-order U_v in A_v, so that $\lambda_v U_v = U_v \lambda_v = P_v$ is the maximal two-sided proper ideal of U_v. For $0 \neq q \in A_v$ there is an integer ℓ such that $qU_v = \lambda_v^{\ell} U_v$, and $|q|_v = |\mathrm{N}_v(\lambda_v^{\ell})|_v^{1/d(v)} = (\#k(v))^{-\ell/d(v)}$. This interpretation of $|q|_v$ implies that $|a| = \max_{i,j}|a_{i,j}|_v$ is unchanged if we multiply a matrix $a = (a_{i,j}) \in \mathrm{M}_{m(v)}(A_v)$ on the left or right by a permutation matrix, by a matrix which multiplies a single row or column by an element of U_v^*, or by an elementary matrix associated with some element of U_v. Thus to prove inequality (2) of Lemma 3.2, we can use these operations to reduce to the case where y is a diagonal matrix with entries $\lambda_v^{z_1}, \ldots, \lambda_v^{z_{m(v)}}$ for some integers $z_1, \ldots, z_{m(v)}$.

When y has this form,

$$|y|_v^{d(v)} = \max\{|\mathrm{N}_v(\lambda_v^{z_i})|_v : 1 \leq i \leq m(v)\} = (\#k(v))^{-\min_i\{z_i\}},$$

$$|\det_v(y)|_v = |\mathrm{N}_v(\lambda)^z|_v = (\#k(v))^{-z} \quad \text{where} \quad z = \sum_{i=1}^{m(v)} z_i,$$

and y^{-1} is the diagonal matrix with entries $\lambda_v^{-z_1}, \ldots, \lambda_v^{-z_{m(v)}}$. Therefore,

$$|y^{-1}|_v^{d(v)} = (\#k(v))^{-\min_i\{-z_i\}} = (\#k(v))^{\max_i\{z_i\}}.$$

The inequality in statement *2.* of the lemma is therefore equivalent to

$$\max_i\{z_i\} - z \leq -(m(v) - 1)\, \min_i\{z_i\}.$$

This is the same as

$$z - \max_i\{z_i\} \geq (m(v) - 1)\min_i\{z_i\},$$

which is certainly true. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Lemma 3.3. *Suppose v is an infinite place, so that there is an isomorphism $\rho_v : B_v \to \mathrm{M}_{m(v)}(A_v)$ with $A_v = k_v$ if v is complex and either $A_v = k_v$ or $A_v = \mathbb{H}$ if v is real. Define $\det'_v : B_v \to k_v$ by $\det'_v(q) = |\det_v(q)|_v^{1/d(v)}$ where $\det_v : B_v \to k_v$ is the reduced norm. Then, there are minimal real constants $\delta_1(A_v, m(v))$ and $\delta_2(A_v, m(v))$ such that for all $y, y' \in B_v$:*

1. *$|yy'|_v \le \delta_1(A_v, m(v)) \, |y|_v \, |y'|_v$.*
2. *$|yy'|_v = |y|_v \, |y'|_v$ if either y or y' is a scalar matrix or a permutation matrix.*
3. *$|\det'_v(y)y^{-1}|_v \le \delta_2(A_v, m(v)) \, |y|_v^{m(v)-1}$ for all $y \in B_v^*$.*

We also have the bounds

$$\text{(17)} \qquad\qquad 1 \le \delta_1(A_v, m(v)) \le m(v)^{[k_v:\mathbb{R}]}$$

$$\text{(18)} \qquad\qquad 1 \le \delta_2(A_v, m(v)) \le 2^{[k_v:\mathbb{R}]m(v)(m(v)-1)}.$$

Furthermore, if $A_v = k_v$ then

$$\text{(19)} \qquad\qquad 1 \le \delta_2(A_v, m(v)) \le ((m(v)-1)!)^{[k_v:\mathbb{R}]}.$$

Proof. As before,

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

where

$$\rho_v(y) = (y^{i,j}(v))_{i,j} \in \mathrm{M}_{m(v)}(A_v)$$

and $|q|_v = |\mathrm{N}_v(q)|_v^{1/d(v)}$ for $q \in A_v$, and where $\mathrm{N}_v : A_v \to k_v$ is the reduced norm and $\dim_{k_v}(A_v) = d(v)^2$. We noted earlier that $|qq'|_v = |q|_v|q'|_v$ for all $q, q \in A_v$, and by Lemma 3.1,

$$\left|\sum_{i=1}^{m(v)} q_i\right|_v \le m(v)^{[k_v:\mathbb{R}]-1} \sum_{i=1}^{m(v)} |q_i|_v \le m(v)^{[k_v:\mathbb{R}]}\max_i\{|q_i|_v\}$$

for $\{q_i\}_i \subset A_v$. By writing the matrix entries of yy' as sums of products of the entries of y and y' this leads to (1) in Lemma 3.3 and the stated bounds on $\delta_1(A_v, m(v))$. The bound (2) in Lemma 3.3 is clear.

Now suppose that $y \in B_v^*$. We can find permutation matrices r and r' such that the entry q of ryr' for which $| \, |_v$ is maximal lies in the upper left corner. We then perform Gauss–Jordan elimination on the rows and columns of ryr' to produce matrices e and e' in $\mathrm{M}_{m(v)}(A_v)$ such that e and e' are products of elementary matrices and the nonzero off-diagonal entry of each elementary matrix for e or e' has the form $-\tau/q$ for some entry τ of ryr', where $|-\tau/q|_v = |\tau|_v/|q|_v \le 1$. The matrix $y_1 = eryr'e'$ has the same entry q as y in the upper left corner, and all of the other entries in the first row and the first column are 0. Finally, the other entries of y_1 have the form $\alpha - (\tau/q)\beta$ where α, β, and τ are entries of ryr'. Since $|\tau|_v \le |q|_v$ we see from Lemma 3.1 that

$$|\alpha - (\tau/q)\beta|_v \le 2^{[k_v:\mathbb{R}]-1}(|\alpha|_v + |\beta|_v) \le 2 \cdot 2^{[k_v:\mathbb{R}]-1}|q|_v = 2^{[k_v:\mathbb{R}]}|y|_v.$$

Since q is an entry of y_1, we deduce that

$$|y|_v \leq |y_1|_v \leq 2^{[k_v:\mathbb{R}]}|y|_v \quad \text{and} \quad \det(y_1) = \pm \det(y).$$

We now continue with y_1 and construct matrices $s, s' \in \mathrm{M}_{m(v)}(A_v)$ such that s and s' are products of elementary matrices and permutation matrices, and the off-diagonal entries of the elementary matrices involved in each product have absolute value with respect to $|\ |_v$ bounded above by 1. The matrix $y' = sys'$ is diagonal and

$$(20) \qquad\qquad\qquad |y|_v \leq |y'|_v \leq 2^{[k_v:\mathbb{R}](m(v)-1)}|y|_v$$
$$(21) \qquad\qquad\qquad \det(y') = \pm \det(y).$$

Then $(y')^{-1} = (s')^{-1}y^{-1}s^{-1}$ and $s'(y')^{-1}s = y^{-1}$, where $s, s', (s')^{-1}$, and s^{-1} are products of elementary matrices and permutation matrices such that the off diagonal entries in each elementary matrix has absolute value with respect to $|\ |_v$ bounded by 1. This leads by the above reasoning to the bounds

$$(22) \qquad\qquad\qquad |(y')^{-1}|_v \leq 2^{[k_v:\mathbb{R}](m(v)-1)}|y^{-1}|_v$$
$$(23) \qquad\qquad\qquad |y^{-1}|_v \leq 2^{[k_v:\mathbb{R}](m(v)-1)}|(y')^{-1}|_v.$$

Write $y' = \mathrm{diag}(c_1, \ldots, c_{m(v)})$ for some $c_i \in A_v$. Define $r_i = |c_i|_v = |\mathrm{N}_v(c_i)|_v^{1/d(v)}$. Then

$$|y'|_v = \max_i\{r_i\},$$

$$\det'(y') = \prod_i r_i = r,$$

$$\det'(y')(y')^{-1} = \mathrm{diag}(rc_1^{-1}, \ldots, rc_{m(v)}^{-1}).$$

We deduce from this that

$$
\begin{aligned}
|\det'(y')(y')^{-1})|_v &= \max_i\{|rc_i^{-1}|_v\} \\
&= r\max_i\{|c_i^{-1}|_v\} \\
(24) \qquad &= r\max_i\{r_i^{-1}\} \\
(25) \qquad &\leq (\max_i\{r_i\})^{m(v)-1} \\
(26) \qquad &= |y'|_v^{m(v)-1}.
\end{aligned}
$$

Combining this with (20) and (22) gives

$$
\begin{aligned}
|\det'(y)(y)^{-1})|_v &= |\det'(y)|_v|y^{-1}|_v \\
&= |\det'(y')|_v|y^{-1}|_v \\
&\leq 2^{[k_v:\mathbb{R}](m(v)-1)}|\det'(y')|_v|(y')^{-1}|_v \\
&\leq 2^{[k_v:\mathbb{R}](m(v)-1)}|\det'(y')(y')^{-1}|_v \\
&\leq 2^{[k_v:\mathbb{R}](m(v)-1)}|y'|_v^{m(v)-1} \\
&\leq 2^{[k_v:\mathbb{R}](m(v)-1)}\left(2^{[k_v:\mathbb{R}](m(v)-1)}|y|_v\right)^{m(v)-1} \\
&= 2^{[k_v:\mathbb{R}]m(v)(m(v)-1)}|y|_v^{m(v)-1}.
\end{aligned}
$$

(27)

This gives (2) in Lemma 3.3 and the bound (18) on $\delta_2(A_v, m(v))$.

Now, suppose that $A_v = k_v$. We can improve the above bound on $\delta_2(A_v, m(v))$ using the fact that $\det(y)y^{-1}$ is the transpose of the cofactor matrix of y. Using the formula for the determinant as a sum over permutations, every entry $\det(y)y^{-1}$ is the sum of $(m(v)-1)!$ terms, each of which is ± 1 times a product of $m(v)-1$ entries of the matrix y. The absolute value with respect to $|\ |_v$ of each entry of y is bounded by $|y|_v$, which implies that

$$
|\det(y)y^{-1}|_v \leq ((m(v)-1)!)^{[k_v:\mathbb{R}]-1}(m(v)-1)!|y|_v^{m(v)-1} =
$$

$$
((m(v)-1)!)^{[k_v:\mathbb{R}]}|y|_v^{m(v)-1}.
$$

This is the bound in (19). $\qquad\square$

4. The main result

We retain all notation and definitions from §§2-3. Let $\{\omega_i\}_{i=1}^{nd^2}$ be a $\mathbb{Z}$-basis for $\mathcal{D}$. The discriminant $d_\mathcal{D}$ of $\mathcal{D}$ is defined to be

$$
d_\mathcal{D} = \det(M),
$$

where M is the matrix $(T(\omega_i\,\omega_j))_{1\leq i,j\leq nd^2}$ and $T: B_\mathbb{R} \to \mathbb{R}$ is the trace. As a real vector space, $B_\mathbb{R} \cong \mathbb{R}^{nd^2}$. The additive Tamagawa measure Vol on B described in [2, §X.3] is defined in such a way that

(28) $$ d_\mathcal{D} = \mathrm{Vol}(B_\mathbb{R}/\mathcal{D}) = |d_\mathcal{D}|^{1/2}. $$

Consider a compact convex symmetric subset X of $B_\mathbb{R}$. By Minkowski's lattice point theorem, if

(29) $$ \mathrm{Vol}(X) \geq 2^{\dim_\mathbb{Q} B}\, d_\mathcal{D}, $$

then X contains a nonzero element of $\mathcal{D}$. Since X is bounded, there is a constant m_X such that $|\mathrm{Norm}_v(y)|_v$ is bounded by $m_X^{[k_v:\mathbb{R}]/n}$ for every $y \in B_v \cap X$ and $v \in V_\infty$. Then the set

(30) $$ F_X = \{(x,\beta) \in G_S \ : \ x \in X, \ \beta\mathcal{D} \subseteq \mathcal{D}, \ [\mathcal{D}:\beta\mathcal{D}] \leq m_X\} $$

is a compact subset of G_S.

Proposition 4.1. *With notation as above, suppose that S contains all finite places v of k such that $|\mathrm{Norm}_{k/\mathbb{Q}}(v)|^d \leq m_X$. Then F_X is a fundamental set for the action of Γ_S on G_S in the sense that $\Gamma_S F_X = G_S$.*

Proof. Given $(x, \beta) \in G_S$, we must show that there exists $c \in \Gamma_S$ such that $(cx, c\beta) \in F_X$. This happens if and only if

$$\text{(31)} \qquad\qquad c\beta\mathcal{D} \quad \subseteq \quad \mathcal{D}$$
$$\text{(32)} \qquad\qquad [\mathcal{D} : c\beta\mathcal{D}] \quad \leq \quad m_X, \quad \text{and}$$
$$\text{(33)} \qquad\qquad cx \quad \in \quad X.$$

By definition, (31) means that $c \in \mathcal{D}\beta^{-1}$. If $cx \in X$, then

$$
\begin{aligned}
[\mathcal{D} : c\beta\mathcal{D}] &= |\mathrm{Norm}_f(c\beta)|^{-1} \\
&= |\mathrm{Norm}_f(c)|^{-1} |\mathrm{Norm}_f(\beta)|^{-1} \\
\text{(34)} \qquad &= |\mathrm{Norm}_\infty(c)| |\mathrm{Norm}_\infty(x)| \\
&= |\mathrm{Norm}_\infty(cx)| \\
&\leq \prod_{v \in V_\infty} m_X^{[k_v:\mathbb{Q}]/n} = m_X
\end{aligned}
$$

by (9) and the definitions of G_S and m_X. Therefore (33) implies (32). Combining these facts, it suffices to show that $\mathcal{D}\beta^{-1} \cap Xx^{-1}$ contains an element of Γ_S.

Since Xx^{-1} is convex and symmetric with volume $\mathrm{Vol}(X)|\mathrm{Norm}_\infty(x)|^{-1}$ and the lattice $\mathcal{D}\beta^{-1}$ in $\mathbb{R}^{nd^2}$ has covolume

$$\mathrm{Covol}(\mathcal{D}\beta^{-1}) = d_{\mathcal{D}}|\mathrm{Norm}_f(\beta^{-1})|^{-1} = d_{\mathcal{D}}|\mathrm{Norm}_\infty(x)|^{-1},$$

this implies that

$$\mathrm{Vol}(Xx^{-1}) \geq 2^{\dim_{\mathbb{Q}} B}\mathrm{Covol}(\mathcal{D}\beta^{-1})$$

if and only if $\mathrm{Vol}(X) \geq 2^{\dim_{\mathbb{Q}} B} d_{\mathcal{D}}$. Since this holds by definition of X, it follows that $Xx^{-1} \cap \mathcal{D}\beta^{-1}$ contains a nonzero element c of $\mathcal{D}\beta^{-1}$. By construction, c is an element of B^* such that $(cx, c\beta) \in F_X$. We claim that $c \in \Gamma_S$.

Since $c\beta \in \mathcal{D}$, it follows from (4) that $|\mathrm{Norm}_v((c\beta)_v)|^{-1}$ is a nonnegative integral power of $\mathrm{Norm}_{k/\mathbb{Q}}(v)^d$ for each $v \in V_f$. We know that

$$\prod_{v \notin V_\infty} |\mathrm{Norm}_v((c\beta)_v)|^{-1} = |\mathrm{Norm}_f(c\beta)|^{-1} = |\mathrm{Norm}_\infty(cx)| \leq m_X$$

by (34). Hence if $|\mathrm{Norm}_v((c\beta)_v)| \neq 1$ for some finite place v, then

$$|\mathrm{Norm}_{k/\mathbb{Q}}(v)|^d \leq m_X,$$

which implies that $v \in S_f$. It follows that

$$|\mathrm{Norm}_v((c\beta)_v)| = 1$$

for all $v \in V_f \smallsetminus S_f$. Thus $(c\beta)_v \mathcal{D}_v = \mathcal{D}_v$ for these v, since $c\beta \in \mathcal{D}$. However, $\beta_v = 1$ if $v \notin S$, so

$$c\mathcal{D}_v = c_v\mathcal{D}_v = (c\beta)_v\mathcal{D}_v = \mathcal{D}_v$$

for all $v \in V_f \smallsetminus S_f$. This implies that $c \in \mathcal{D}_v^*$ for all $v \notin S_f$, so $c \in \Gamma_S$. This proves the proposition. $\qquad\square$

We now describe how F_X determines generators for Γ_S. A subset P of G_S will be called a set of *topological generators* for G_S if for any open subset O of G_S, the group generated by O and P is all of G_S. The following lemma should be compared with [7, Lemma 6.3].

Lemma 4.2. *Let P be a set of topological generators for G_S that contains the identity, and let F_X be as in Proposition 4.1. Then Γ_S is generated by its intersection with $F_X P F_X^{-1}$.*

Proof. We have an equality of sets

$$F_X(P \cup P^{-1})F_X^{-1} = (F_X P F_X^{-1}) \cup (F_X P F_X^{-1})^{-1}.$$

Therefore we can replace P by $P \cup P^{-1}$ for the remainder of the proof and assume that P is symmetric, i.e., that $P = P^{-1}$. We emphasize that this does not mean we must assume P is symmetric in the statement of the lemma.

Consider the subset

$$O = (G_S \smallsetminus \Gamma_S) \cup (\Gamma_S \cap F_X F_X^{-1})$$

of G_S. This is an open neighborhood of $F_X F_X^{-1}$ in G_S because Γ_S is a discrete subgroup of G_S. Since F_X is a fundamental set for the action of Γ_S on G_S, we can find a subset $F \subset F_X$ such that $\Gamma_S \times F \to G_S$ is a bijection. We claim that there is a small open neighborhood U of the identity in G_S such that $FUF^{-1} \subset O$.

It will be enough to find a U such that $\Gamma_S \cap (FUF^{-1}) \subset F_X F_X^{-1}$. Let T be the set of $\gamma \in \Gamma_S$ such that $\gamma F \cap FU \neq \emptyset$. We want to show that if $\gamma \in T$, then $\gamma F_X \cap F_X \neq \emptyset$. Since F is a bounded fundamental domain for the action of Γ_S on G_S and Γ_S is discrete in G_S, the set T is finite when U is bounded. We can then shrink U further and assume that if $\gamma \in T$, then $\gamma F' \cap F' \neq \emptyset$ for each open neighborhood F' of the closure of F in G_S. If $\gamma F_X \cap F_X = \emptyset$ for some $\gamma \in T$, then since F_X is compact there will be an open neighborhood F' of F_X for which $\gamma F' \cap F' = \emptyset$. This is a contradiction, since the closure of F is contained in F_X, which proves the claim.

Let $P' = P \cup U$, so $\langle P' \rangle = G_S$, and let $\Delta < \Gamma_S$ be the subgroup generated by $\Gamma_S \cap FP'F^{-1}$. We claim that $\Delta = \Gamma_S$. Indeed, if $xp \in FP'$, there exist $y \in F$ and $\gamma \in \Gamma_S$ such that $xp = \gamma y$. Then

$$\gamma = xpy^{-1} \in FP'F^{-1},$$

so $\gamma \in \Delta$. This implies that $FP' \subseteq \Delta F$, so $\Delta FP' \subseteq \Delta F$. Therefore, ΔF is right P'-invariant, but $\langle P' \rangle = G_S$, so $\Delta F = G_S$. Since $\Gamma_S \times F \to G_S$ is a bijection, it follows that $\Delta = \Gamma_S$.

This proves that Γ_S is generated by

$$\Gamma_S \cap FP'F^{-1} \subseteq (\Gamma_S \cap FPF^{-1}) \cup (\Gamma_S \cap FUF^{-1}).$$

However, $FUF^{-1} \subset O$, and $\Gamma_S \cap O \subset F_X F_X^{-1}$ by definition, so

$$(35) \qquad \Gamma_S \cap FP'F^{-1} \subseteq (\Gamma_S \cap F_X P F_X^{-1}) \cup (\Gamma_S \cap F_X F_X^{-1}).$$

Since P contains the identity, the right side of (35) equals $\Gamma_S \cap F_X P F_X^{-1}$. This proves the lemma. $\square$

We now define several constants that we need to state our main result.

(1) For X, F_X, and ℓ as above, let T_1 be the supremum of 1 and

$$\left\{ |x_v|_v^{d(v)/[k_v:\mathbb{R}])} \right\}$$

over all

$$x = \prod_{v \in V_\infty} x_v \in B_\mathbb{R}$$

for which $(x, \beta) \in F_X$ for some β.

(2) Let P be a finite set of topological generators for G_S which contains the identity element (see §5.4 for an example of such a set). We assume that every element of P has the form (z, ζ) with $z = \prod_{v \in S_\infty} z_v \in B_\mathbb{R}^*$ and $\zeta = \prod_{v \in S_f} \zeta_v \in B_{S_f}^*$, where z_v is a real scalar and each ζ_v lies in the local maximal order $\mathrm{M}_{m(v)}(U_v)$ of $B_v = \mathrm{M}_{m(v)}(A_v)$ (cf. §5.4). Let T_2 be the supremum of 1 and

$$\left\{ |z_v|_v^{d(v)/[k_v:\mathbb{R}]} \right\}$$

over all $z = \prod_v z_v \in P$ and all $v \in V_\infty$.

(3) Let T_3 be

$$\prod_{v \in S_f} \max \left\{ 1, |\alpha_v|_v^{d(v)} \right\}$$

where as (x, α) ranges over F_X and $\alpha = \prod_{v \in S_f} \alpha_v \in B_{S_f}^*$. Note that for such α and α_v we have that $\alpha_v \mathcal{D}_v \subseteq \mathcal{D}_v$. Such α_v are contained in $\mathcal{D}_v$, so this constant is finite. Similarly, define T_3' to be the maximum of

$$\prod_{v \in S_f} \max \left\{ 1, |\alpha_v|_v^{d(v)(m(v)-1)} \right\},$$

where α and the α_v range as above.

(4) Let T_4 be the smallest number such that

$$\prod_{v \in S_f} \max \left\{ 1, |g_v|_v^{d(v)} \right\} \leq T_4$$

for all $g = \prod_v g_v \in P$.

(5) Let T_5 be the supremum of 1 and

$$\left\{ |\det_v(a_v)|_v^{1/[k_v:\mathbb{R}]} \; : \; a \in F_X \text{ and } v \in V_\infty \right\}.$$

where we write $a \in F_X$ as $a = (a_v)_v$ with $a_v \in B_v$. (Recall that $\det_v : B_v \to k_v$ is the reduced norm.)

(6) Let T_6 be the maximum over all subsets W of V_∞ of

$$T_1^{a(W)} T_2^{b(W)} T_5^{b(V_\infty \smallsetminus W)}$$

where

(36) $$a(W) = \sum_{v \in W} [k_v : \mathbb{R}] m(v) \quad \text{and} \quad b(W) = \sum_{v \in W} [k_v : \mathbb{R}].$$

Now we are ready to state and prove our main result.

Theorem 4.3. *Let k be an algebraic number field of degree n over $\mathbb{Q}$ and B a central simple k-division algebra of degree d. Let S be a finite set of places of k containing all the archimedean places V_∞ and let $\mathcal{D} \subset B$ be an O_k-order. We suppose that the k_v isomorphisms $\rho_v : B_v \to \mathrm{M}_{m(v)}(A_v)$ are chosen such that $\rho_v(\mathcal{D}_v) \subseteq \mathrm{M}_{m(v)}(U_v)$ for $v \notin S$, where U_v is the unique maximal O_v-order in the k_v-division algebra A_v. Suppose s is the number of (real) places v at which A_v is isomorphic to $\mathbb{H}$. Let G_S be the topological group defined in (9), P be a topological generating set for G_S satisfying the above conditions, and let Γ_S be the group of S-units associated with $\mathcal{D}$.*

Suppose that X is a convex symmetric subset of $B_\mathbb{R}$ such that (29) holds, and let m_X be the smallest real number such that $|\mathrm{Norm}_v(y)|_v$ is bounded by $m_X^{[k_v:\mathbb{R}]/n}$ for every $y \in B_v \cap X$ and $v \in V_\infty$. Suppose that S contains every finite place v of k such that $\mathrm{Norm}(v) \le m_X^{1/d}$. Finally, let $T_1, \ldots, T_6$ be the constants defined immediately above.

Then the set $\Gamma_S \cap F_X P F_X^{-1}$ from Lemma 4.2 is contained in

(37) $$\mathfrak{G}_{S,X} = \mathrm{BH}_S \left(((d-1)!d)^n \left(\frac{2^{(d/2)(d-2)}d}{4(d-1)!} \right)^s T_6 T_3 T_3' T_4 \right).$$

Consequently, $\mathfrak{G}_{S,X}$ is a finite generating set for Γ_S.

Proof. Suppose that $\gamma \in \Gamma_S \cap F_X P F_X^{-1}$. Then, there exist elements $(z, \zeta) \in P$ and

$$(x, \alpha), (y, \beta) \in F_X, \quad x, y \in X, \quad \alpha = \prod_{v \in S_f} \alpha_v, \; \beta = \prod_{v \in S_f} \beta_v$$

so that $(\gamma, \gamma) = (x, \alpha)(z, \zeta)(y^{-1}, \beta^{-1})$. That is, $x_v z_v y_v^{-1} = \gamma$ for each $v \in V_\infty$ and $\alpha_v \zeta_v \beta_v^{-1} = \gamma$ for each $v \in S_f$.

Let $W(\gamma) = W_\infty(\gamma) \cup W_f(\gamma)$ be the set of places v of k at which $|\gamma|_v > 1$. By assumption, if $v \notin S$, then v is finite and $\rho_v(\mathcal{D}_v) \subseteq \mathrm{M}_{m(v)}(U_v)$. Thus $\gamma \in \Gamma_S$ implies that $|\gamma|_v \le 1$ if $v \notin S$. Thus $W(\gamma) \subseteq S$, $W_\infty(\gamma) \subset V_\infty$ and $W_f(\gamma) \subseteq S_f$.

By definition of $H(\gamma)$ we have

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

Recall that $\det_v : B_v \to k_v$ is the reduced norm and that $d(v)^2$ is the dimension of A_v over k_v. If v is archimedean, we defined $\det_v' : B_v \to k_v$ by $\det_v'(q) = |\det_v(q)|_v^{1/d(v)}$ for $q \in B_v$.

We have $|c\alpha|_v = |c|_v |\alpha|_v$ for $c \in k_v$ and $\alpha \in B_v$, where $|c|_v$ here denotes the absolute value of $c \in k_v$ with respect to $|\ |_v : k_v \to \mathbb{R}$. Therefore we can rewrite the above expression as

$$(38) \qquad H(\gamma) = \prod_{v \in W_\infty(\gamma)} |\det_v'(y_v) x_v z_v y_v^{-1}|_v^{d(v)}$$

$$(39) \qquad \times \prod_{v \in W_f(\gamma)} \left(|\det_v(\beta_v)|_v \, |\alpha_v \zeta_v \beta_v^{-1}|_v^{d(v)} \right)$$

$$(40) \qquad \times \prod_{v \in W_\infty(\ \gamma)} |\det_v(y_v)|_v^{-1}$$

$$(41) \qquad \times \prod_{v \in W_f(\gamma)} |\det_v(\beta_v)|_v^{-1},$$

where the last two products are computed using the absolute values on the completions k_v. We now proceed to bound each of these terms.

Sublemma 1. *One has that*

$$(42) \qquad \prod_{v \in W_\infty(\gamma)} |\det_v'(y_v)(x_v z_v y_v^{-1})|_v^{d(v)} \le \mu_1 \, T_1^{a(W_\infty(\gamma))} \, T_2^{b(W_\infty(\gamma))}$$

where $a(W_\infty(\gamma))$ and $b(W_\infty(\gamma))$ are as in (36) and

$$(43) \qquad \mu_1 = \prod_{v \in W_\infty(\gamma)} \delta_1(A_v, m(v))^{d(v)} \delta_2(A_v, m(v))^{d(v)}.$$

Furthermore,

$$(44) \qquad \mu_1 \le ((d-1)!d)^{[k:\mathbb{Q}]} \left(\frac{2^{(d/2)(d-2)}d}{4(d-1)!} \right)^s.$$

if $A_v = \mathbb{H}$ at exactly s real places of k.

Proof. By assumption each z_v is a real scalar. Therefore, Lemma 3.3 gives

$$|\det_v'(y_v)(x_v z_v y_v^{-1})|_v^{d(v)}$$

$$(45) \quad \le \delta_1(A_v, m(v))^{d(v)} |x_v|_v^{d(v)} |z_v|_v^{d(v)} |\det_v'(y_v) y_v^{-1}|_v^{d(v)}$$

$$\le \delta_1(A_v, m(v))^{d(v)} |x_v|_v^{d(v)} |z_v|_v^{d(v)} \delta_2(A_v, m(v))^{d(v)} |y_v|_v^{d(v)(m(v)-1)}$$

$$\le \delta_1(A_v, m(v))^{d(v)} \delta_2(A_v, m(v))^{d(v)} T_1^{[k_v:\mathbb{R}]} T_2^{[k_v:\mathbb{R}]} T_1^{[k_v:\mathbb{R}](m(v)-1)}$$

Taking the product over all $v \in W_\infty(\gamma)$, we get (42) and (43) because $T_1, T_2 \geq 1$. To prove the bound in (44) we first note that $(m(v), d(v)) = (d, 1)$ if v is archimedean and $A_v = k_v$, while $(m(v), d(v)) = (d/2, 2)$ if $k_v = \mathbb{R}$ and $A_v = \mathbb{H}$. By Lemma 3.3,

$$\delta_1(A_v, m(v))^{d(v)} \delta_2(A_v, m(v))^{d(v)} \leq d^{[k_v:\mathbb{R}]}(d-1)!^{[k_v:\mathbb{R}]}$$

if $A_v = k_v$ and

$$\delta_1(A_v, m(v))^{d(v)} \delta_2(A_v, m(v))^{d(v)} \leq (d/2)^{2[k_v:\mathbb{R}]} 2^{[k_v:\mathbb{R}](d/2)(d-2)}$$

when $A_v = \mathbb{H}$. Since $\delta_1(A_v, m(v)) \geq 1$ and $\delta_2(A_v, m(v)) \geq 1$ for all archimedean v, and $[k_v : \mathbb{R}] = 1$ if $A_v = \mathbb{H}$ we see that

$$\mu_1 = \prod_{v \in W_\infty(\gamma)} \delta_1(A_v, m(v))^{d(v)} \delta_2(A_v, m(v))^{d(v)}$$

$$\leq \prod_{v \in V_\infty} \delta_1(A_v, m(v))^{d(v)} \delta_2(A_v, m(v))^{d(v)}$$

$$(46) \qquad \leq \left(\prod_{v \in V_\infty} ((d-1)!d)^{[k_v:\mathbb{R}]} \right) \left(\frac{(d/2)^2 2^{(d/2)(d-2)}}{(d-1)!d} \right)^s.$$

This gives (44) since $\sum_{v \in V_\infty} [k_v : \mathbb{R}] = n$. $\qquad \square$

Sublemma 2.

$$(47) \qquad \prod_{v \in W_f(\gamma)} \left(|\det_v(\beta_v)|_v \, |(\alpha_v \zeta_v \beta_v^{-1})|_v^{d(v)} \right) \leq T_3 T_4 T_3' \leq T_3^d T_4.$$

Proof. By Lemma 3.2, for every $v \in W_f(\gamma)$ we have that

$$|\det_v(\beta_v)|_v \, |(\alpha_v \zeta_v \beta_v^{-1})|_v^{d(v)} \leq |\alpha_v|_v^{d(v)} |\zeta_v|_v^{d(v)} |\det_v(\beta_v)|_v |\beta_v^{-1}|_v^{d(v)}$$

$$(48) \qquad\qquad\qquad \leq |\alpha_v|_v^{d(v)} |\zeta_v|_v^{d(v)} |\beta_v|_v^{d(v)(m(v)-1)}.$$

We take the product of these bounds over $v \in W_f(\gamma)$ to deduce (47). $\qquad \square$

Sublemma 3.

$$\prod_{v \in W_\infty(\gamma)} |\det_v(y_v)|_v^{-1} \leq |\mathrm{Norm}_\infty(y)|^{-1/d} T_5^{b(V_\infty \setminus W_\infty(\gamma))}.$$

Proof. We have

$$\prod_{v \in W_\infty(\gamma)} |\det_v(y_v)|_v^{-1} = \frac{1}{|\mathrm{Norm}_\infty(y)|^{1/d}} \prod_{v \in V_\infty \setminus W_\infty(\gamma)} |\det_v(y_v)|_v.$$

since Norm_∞ is associated with the dth power of the reduced norm. Since $y \in F_X$, by the definition of T_5 we have $|\det(y_v)|_v \leq T_5^{[k_v:\mathbb{R}]}$ for all $v \in V_\infty$, so the lemma is clear. $\qquad \square$

Sublemma 4.

$$\prod_{v \in W_f(\gamma)} |\det_v(\beta_v)|_v^{-1} \leq |\mathrm{Norm}_f(\beta)|^{-1/d} = |\mathrm{Norm}_\infty(y)|^{1/d}$$

Proof. Recall that $(y, \beta) \in F_X$, so that $\beta \mathcal{D} \subset \mathcal{D}$. Since $\mathcal{D}$ is a O_k-lattice in B, this implies that all the components of $\beta = \prod_{v \in S_f} \beta_v \in B_f^*$ are integral over O_k. We view β an idele in $J(B)$ with component 1 outside of S_f. Since $\det_v : B_v \to k_v$ is the reduced norm, we conclude that $|\det_v(\beta_v)|_v \le 1$ for all places v of k. We now have

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

$$\le \prod_{v \in V_f} |\det_v(\beta_v)|_v^{-1} = |\mathrm{Norm}_f(\beta)|^{-1/d}.$$

The second equality in the statement of the sublemma follows from the definition of $(y, \beta) \in G_S$. $\qquad \square$

Substituting these bounds in (38)–(41) shows that γ lies in (37) and completes the proof of Theorem 4.3. $\qquad \square$

Remark 1. Notice that we used the fact that B is a division algebra to ensure that Minkowski's theorem returns an invertible element of B. It would be interesting to prove an analogue of our result for S-unit groups of any central simple algebra over a number field. Given that $\mathrm{SL}_n(\mathbb{Z})$ is generated by elementary matrices, which certainly have small height, we expect such a result to hold.

5. Explicit bounds

In this section we make some particular choices in order to give more explicit calculations of the bounds in the previous section.

As before, B is a division algebra of dimension d^2 with center a number field k of degree $n = [k : \mathbb{Q}]$ over $\mathbb{Q}$. Let $V = V_\infty \cup V_f$ be the set of places of k, r_1 the number of real places of k, and r_2 the number of complex places. For $v \in V$, we fix an isomorphism of B_v with $\mathrm{M}_{m(v)}(A_v)$ where A_v is a division algebra of dimension $d(v)^2$ over its center k_v.

5.1. A maximal order $\mathcal{D}$ and an archimedean set X. Suppose that $\mathcal{D}$ is the maximal order of B that is isomorphic to $\mathrm{M}_{m(v)}(U_v)$ for all finite v, where U_v is the unique maximal O_v order in A_v.

Suppose first that v is archimedean. The normalized Haar measure on k_v is the Euclidean measure if $k_v = \mathbb{R}$ and is twice the Euclidean measure if $k_v = \mathbb{C}$. The normalized Haar measure on $\mathbb{H} = \mathbb{R} + \mathbb{R}I + \mathbb{R}J + \mathbb{R}IJ$ is 4 times the one associated to the usual Euclidean measure on $\mathbb{R}^4$ under the basis $\{1, I, J, IJ\}$. The norm on $\mathbb{H}$ is $|\alpha| = |N(\alpha)|^{1/2}$ where $N : \mathbb{H} \to \mathbb{R}$ is the reduced norm. Thus the volume with respect to the normalized Haar measure of a ball of radius $c^{1/2}$ inside $\mathbb{H}$ is

$$4\frac{\pi^2}{\Gamma(3)}c^2 = 2\pi^2 c^2.$$

The normalized volume of a ball of radius c in $\mathbb{C}$ (resp. $\mathbb{R}$) is $2\pi c^2$ (resp. $2c$). The normalized Haar measure on $B_v = \mathrm{M}_{m(v)}(A_v)$ is then the product measure associated with matrix entries. Here $(m(v), d(v)) = (d, 1)$ if $A_v = k_v$ and $(m(v), d(v)) = (d/2, 2)$ if $A_v = \mathbb{H}$, and there are $m(v)^2$ matrix entries associated to each element of B_v.

Let $S_{ram,\infty}(B)$ be the set of infinite places of k at which B ramifies. Recall that $s = \#S_{ram,\infty}(B)$. We have $\dim_{k_v}(A(v)) = d(v)^2$, so $d(v) = 1$ or 2 if v is infinite. Let $c > 1$ be a real parameter, and let $X(c)$ be the set of

$$x = \prod_{v \in V_\infty} x_v \in B_{\mathbb{R}} = \prod_{v \in V_\infty} B_v$$

such that $|x|_v^{d(v)/[k_v:\mathbb{R}]} \leq c$ for all $v \in V_\infty$. Then

$$\mathrm{Vol}(X(c)) = (2c)^{d^2(r_1-s)} \left(2\pi^2 c^2\right)^{(d/2)^2 s} \left(2\pi c^2\right)^{d^2 r_2} = zc^{d^2(n-s/2)}$$

where

(49) $$z = 2^{d^2(r_1-s)} \left(2\pi^2\right)^{(d/2)^2 s} \left(2\pi\right)^{d^2 r_2}.$$

Now choose c such that

(50) $$zc^{d^2(n-s/2)} = \mathrm{Vol}(X(c)) = 2^{\dim_{\mathbb{Q}} B} \, d_{\mathcal{D}} = 2^{d^2 n} \, d_{\mathcal{D}}.$$

In other words,

(51) $$c = \left(\frac{2^{d^2 n}}{z} d_{\mathcal{D}}\right)^{\frac{1}{d^2(n-s/2)}} = \left(\frac{2}{\pi}\right)^{\frac{r_2}{n-s/2}} \left(\frac{2\sqrt{2}}{\pi}\right)^{\frac{s}{2n-s}} d_{\mathcal{D}}^{\frac{1}{d^2(n-s/2)}}.$$

5.2. The constant m_X. Setting $X = X(c)$, we need to find an m_X such that

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

for all $v \in V_\infty$, where

$$y = \prod_{v \in V_\infty} y_v \in X(c).$$

and $\det_v : B_v \to k_v$ is the reduced norm.

5.2.1. Real v with $A_v = k_v$. In this case $\det_v(y_v)$ is the determinant of a real $d \times d$ matrix each of whose entries is bounded by c in absolute value. The Euclidean length of each column of y_v is thus bounded by dc, so we have

(53) $$|\mathrm{Norm}(y_v)|_v = |\det_v(y_v)|_v^d \leq ((cd)^d)^d = (cd)^{d^2}$$

whenever $k_v = A_v = \mathbb{R}$.

5.2.2. Real v with $A_v = \mathbb{H}$. We have a representation

$$(54) \qquad\qquad \mathbb{H} = \mathbb{R} + \mathbb{R}I + \mathbb{R}J + \mathbb{R}IJ \to M_2(\mathbb{C})$$

determined by

$$I \to \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad J \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad IJ \to \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

This sends $y_v \in M_{d/2}(\mathbb{H})$ to a matrix $y'_v \in M_d(\mathbb{C})$ which consists of 2×2 blocks of the form

$$\begin{pmatrix} \lambda & \mu \\ -\overline{\mu} & \overline{\lambda} \end{pmatrix}$$

for $\lambda, \mu \in \mathbb{C}$.

Since $y_v \in X(c)$, we must have $|y_v|_v^{d(v)} = |y_v|_v^2 \leq c$, where $|y_v|_v^2$ is the supremum of $|\lambda|^2 + |\mu|^2$ over the above 2×2 blocks. The columns of y'_v are vectors $y'_v(1), \ldots, y'_v(d)$ in $\mathbb{C}^d$ with the property that with respect to the usual Hermitian inner product $\langle\ ,\ \rangle$ on $\mathbb{C}^d$ we have

$$\langle y'_v(i), y'_v(i) \rangle \leq dc/2 \quad \text{and} \quad \langle y'_v(2j-1), y'_v(2j) \rangle = 0$$

for $1 \leq i \leq d$ and $1 \leq j \leq d/2$.

Let T be the subset of $\mathbb{C}^d$ consisting of all linear combinations of the form $\sum_{i=1}^d \tau_i y'_v(i)$, where $|\tau_i|_\mathbb{C} \leq 1$ and $|\ |_\mathbb{C}$ is the usual Euclidean inner product on $\mathbb{C}$. Recall that the normalized Haar measure on $\mathbb{C}$ is 2 times the standard Euclidean Haar measure. Give $\mathbb{C}^d$ the product measure. Then T is the image of the unit polydisc in $\mathbb{C}^d$ under left multiplication by the matrix y'_v. Therefore

$$(55) \qquad\qquad \mathrm{Vol}(T) = |\det(y')|_\mathbb{C}^2 (2\pi)^d.$$

On the other hand, T is contained in the product of real two-dimensional metric disks T_i defined by

$$T_i = \{\tau_i\ y'_v(i) : |\tau_i| \leq 1\}$$

as i ranges over $1 \leq i \leq d$. The square Euclidean length $\langle y'_v(i), y'_v(i) \rangle$ of each $y'_v(i)$ is bounded by $dc/2$. We conclude from this that

$$(56) \qquad\qquad \mathrm{Vol}(T) \leq (2\pi dc/2)^d.$$

The reduced norm $\det_v(y_v)$ is equal to $\det(y'_v)$, so (55) and (56) give

$$(57) \qquad |\mathrm{Norm}_v(y_v)|_v = |\det_v(y_v)|_v^d = |\det(y')|_\mathbb{C}^d \leq (dc/2)^{d^2/2}$$

when $k_v = \mathbb{R}$ and $A_v = \mathbb{H}$.

5.2.3. Complex v. Finally suppose $k_v = A_v = \mathbb{C}$. We can define $y_v' = y_v$ and use the above arguments to bound $|\mathrm{Norm}_v(y_v)|_v = |\det(y_v')|_{\mathbb{C}}^{2d}$. Here the columns of y_v' have complex square length bounded by dc^2 since $|y_v|_v^{1/2} \leq c$ in this case, where $|y_v|_v$ is the supremum of the normalized absolute value with respect to $|\ |_v$ of the matrix coefficients of $y_v = y_v'$, and $|\ |_v$ is $|\ |_{\mathbb{C}}^2$. Using the same set T defined above leads to

$$\mathrm{Vol}(T) = |\det(y')|_{\mathbb{C}}^2 (2\pi)^d \leq (2\pi dc^2)^d.$$

We see from this that

(58) $$|\mathrm{Norm}_v(y_v)|_v = |\det(y')|_{\mathbb{C}}^{2d} \leq (dc^2)^{d^2}$$

when $k_v = \mathbb{C} = A_v$.

5.2.4. A choice for m_X. We can now put together (56), (57), and (58) to find a constant m_X that satisfies (52). One can take

$$m_X = \max\left\{ (cd)^{d^2}, (dc/2)^{d^2/2}, (dc^2)^{d^2/2} \right\}^n$$

$$= \max\left\{ cd, (dc/2)^{1/2}, d^{1/2}c \right\}^{nd^2}$$

$$= \max\left\{ cd, (dc/2)^{1/2} \right\}^{nd^2}$$

(59) $$= \begin{cases} (cd)^{nd^2} & \text{if } 2cd \geq 1 \\ (cd/2)^{nd^2/2} & \text{if } 2cd < 1. \end{cases}$$

5.3. Choices for T_1, T_5, T_3 and T_3'. We can take

(60) $$T_1 = \max(1, c)$$

by definition of T_1 and of $X = X(c)$.

By definition of m_X we know that

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

for every $v \in V_\infty$ and $y = \prod_{v \in V_\infty} y_v \in X$. Here $\det_v(y_v)^d = \mathrm{Norm}_v(y_v)$ so

$$|\det_v(y_v)|_v^{1/[k_v:\mathbb{R}]} \leq m_X^{1/(dn)}$$

for v and y as above. It follows from the definition of T_5 that we can take

(61) $$T_5 = \max(1, m_X^{1/(dn)}).$$

We chose $\mathcal{D}$ such that $\mathcal{D}_v$ is $\mathrm{M}_{m(v)}(U_v)$ for every $v \in S_f$, where U_v is the the unique maximal O_v-order in the division algebra A_v. It follows that we can take

(62) $$T_3 = T_3' = 1.$$

5.4. Topological generators and the constants T_2 and T_4. We now specify a set P of topological generators for G_S which contains the identity element. If v is archimedean, then B_v^* is isomorphic to $\mathrm{GL}_d(k_v)$ or $\mathrm{GL}_{d/2}(\mathbb{H})$. We claim that there is a set P_∞ of topological generators for $G_S \cap (B_\mathbb{R}^* \times \{1\})$ consisting of elements of the form $(x, 1) \in (B_\mathbb{R}^* \times B_f^*)$ with $x = \prod_{v \in V_\infty} x_v$ and $|x_v|_v = 1$ for all $v \in V_\infty$.

Indeed, if $A_v = \mathbb{H}$ or $\mathbb{C}$, then $\mathrm{GL}_{m(v)}(A_v)$ is connected, so any open subset of B_v generates all of B_v. Therefore, the only element needed for these places is the identity. If $A_v = \mathbb{R}$, then B_v has two connected components, determined by the sign of the determinant. Here it suffices to take a topological generator in G_S consisting of the matrix $\mathrm{diag}(-1, 1, \ldots, 1)$ at v and the identity at all other v (finite or infinite), which suffices since any open set generates the connected component of the identity. Clearly $|x_v|_v = 1$ for every $x \in P_\infty$ and $v \in V$. This proves the claim.

Now consider v in S_f. Then D_v is isomorphic to $\mathrm{M}_{m(v)}(U_v)$ and B_v is isomorphic to $\mathrm{M}_{m(v)}(A_v)$. Let λ_v be a prime element of D_v, so that $\lambda_v U_v = U_v \lambda_v$ is the unique maximal two-sided proper ideal of U_v.

Include in P_v the set of elements of the form $(1, \beta) \in (B_\mathbb{R}^* \times B_f^*)$ such that $\beta = \prod_{w \in S_f} \beta_w$ has $\beta_w = 1$ unless $w = v$, and β_v is either a permutation matrix, an elementary matrix associated to an element of U_v, or a diagonal matrix having all diagonal elements equal to 1 and the remaining diagonal entry in U_v^*. As in the proof of Lemma 3.2, every element of $B_\mathbb{R}^* \times B_f^*$ can be written as the product of an element in the closure of the group generated by $\cup_{v \in S_f} P_v$ times an element (x, α) in which $x \in B_\mathbb{R}^*$ and $\alpha = \prod_{v \in V_f} \alpha_v \in B_f^*$ has the property that for each $v \in V_f$, there are integers $z_1, \ldots, z_{m(v)}$ which may depend on v such that α_v is the diagonal matrix with diagonal entries $\lambda_v^{z_1}, \ldots, \lambda_v^{z_{m(v)}}$.

Assume that for each $v \in S_f$, P_v contains elements of the form $(x(v), t(v))$, where $t(v) = \prod_{w \in S_f} t(v)_w$ with $t(v)_w = 1$ if $w \neq v$ and $t(v)_v \in B_f^*$ is the diagonal matrix at the place v having one diagonal entry equal to λ_v and the others equal to 1. Let $x(v) \in B_\mathbb{R}^*$ be a real scalar $\tau > 0$ times the identity matrix such that

$$|\mathrm{Norm}_\infty(x(v))| = \tau^{d^2 n} = |\mathrm{Norm}_f(t(v))|^{-1} = (\#k(v))^d.$$

Now the P_w for each $w \in S_f$ together with P_∞ determines a set P of topological generators (x, β) for G_S such that for each archimedean place v we have

(63) $$|x|_v^{d(v)/[k_v:\mathbb{R}]} \leq (m'_{S_f})^{1/n},$$

where $m'_{S_f} = 1$ if $S_f = \emptyset$ and otherwise

(64) $$m'_{S_f} = \max\left\{ (\#k(w))^{d(v)/d} : w \in S_f, v \in S_\infty \right\}.$$

Define m_{S_f} to be 1 when $S_f = \emptyset$ and otherwise

(65) $\qquad m_{S_f} = \max\{\mathrm{Norm}(w) : w \in S_f\} = \max\{\#k(w) : w \in S_f\}.$

Since $d(v) \leq 2$ and $d(v)/d \leq 1$ for $v \in V_\infty$ we have

(66) $\qquad |x|_v^{d(v)/[k_v:\mathbb{R}]} \leq (m'_{S_f})^{1/n} \leq m_{S_f}^{q/n}$ when $q = \min(2/d, 1).$

Therefore we can choose

(67) $$T_2 = (m'_{S_f})^{1/n} \leq m_{S_f}^{q/n}.$$

Since all of the non-archimedean components of elements of P are integral, we can choose

(68) $$T_4 = 1.$$

5.5. An upper bound on T_6. Recall that T_6 is the maximum over all subsets W of V_∞ of

$$T_1^{a(W)} T_2^{b(W)} T_5^{b(V_\infty \smallsetminus W)}$$

where $a(W) = \sum_{v \in W}[k_v : \mathbb{R}]m(v)$ and $b(W) = \sum_{v \in W}[k_v : \mathbb{R}]$. Since

$$T_2 = (m'_{S_f})^{1/n} \geq 1;$$

$$b(W) \leq b(V_\infty) = n;$$

$$T_1 = \max\{1, c\};$$

$$T_5 = \max\{1, m_X^{1/dn}\},$$

we have an upper bound

$$T_1^{a(W)} T_2^{b(W)} T_5^{b(V_\infty \smallsetminus W)}$$

(69) $$\leq \max\{1, c\}^{a(W)} m'_{S_f} \max\{1, m_X\}^{b(V_\infty \smallsetminus W)/dn}.$$

If $2cd < 1$, then $c < 1$ and $m_X < 1$ by (59), so

$$T_1^{a(W)} T_2^{b(W)} T_5^{b(V_\infty \smallsetminus W)} \leq m'_{S_f} \quad \text{if} \quad 2cd < 1.$$

Now suppose that $2cd \geq 1$, so that $m_X = (cd)^{nd^2}$ by (59). Then $m(v) \leq d$ for all $v \in V_\infty$, so (69) gives

$$T_1^{a(W)} T_2^{b(W)} T_5^{b(V_\infty \smallsetminus W)}$$

$$\leq \max\{1, c\}^{db(W)} m'_{S_f} (cd)^{nd^2 b(V_\infty \smallsetminus W)/dn}$$

$$\leq \min\{1, c\}^{db(W)} c^{db(W)+db(V_\infty \smallsetminus W)} m'_{S_f} d^{db(V_\infty \smallsetminus W)}$$

(70) $$\leq c^{nd} m'_{S_f} d^{dn} \quad \text{if} \quad 2cd > 1.$$

Putting together (69) and (70) gives

(71) $$T_6 \leq m'_{S_f} \max\{1, (cd)^{nd}\}.$$

5.6. The explicit bound. Collecting all the above choices leads via Theorem 4.3 to the following result.

Theorem 5.1. *Suppose B is a central simple division algebra of dimension d^2 over a number field k, $n = [k : \mathbb{Q}]$, and s is the number of real places of k over which B ramifies. Then there is a maximal order $\mathcal{D}$ of B and functions $f_1(n, d)$ and $f_2(n, d)$ of integer variables n and d for which the following is true. Define*

$$e = \frac{2n}{d(2n - s)}.$$

Then $e \leq 1$. Suppose that S is a finite set of places of k containing all the archimedean places and that S contains all finite places v such that

$$\mathrm{Norm}(v) \leq f_1(n, d)\, d_{\mathcal{D}}^e.$$

Let m_{S_f} be the maximum norm of a finite place in S. Then the group Γ_S of S-units in B with respect to the order $\mathcal{D}$ is generated by the finite set of elements of height bounded above by

$$f_2(n, d)\, m'_{S_f}\, d_{\mathcal{D}}^e \leq f_2(n, d)\, m_{S_f}\, d_{\mathcal{D}}^e,$$

where m'_{S_f} is as in §5.4. In particular, for fixed n and d, the height bound for the generating set is polynomial in m_{S_f} and $d_{\mathcal{D}}$.

Proof. It is clear that $e = 1/d \leq 1$ if $s = 0$, so suppose that $s > 0$. Then $s \leq n$ and $d \geq 2$ so we again find that $e \leq 1$. The rest of the theorem follows immediately from Theorem 4.3 and the calculations of the previous subsections. $\square$

Remark 2. We now give closed expressions for $f_1(n, d)$ and $f_2(n, d)$ in the case where $c \geq 1$, with c as in (51). We leave the adjustments when $c < 1$ as an exercise. We have

$$(72) \qquad f_1(n, d) = d^{nd} \left(\frac{2}{\pi}\right)^{\frac{ndr_2}{n - s/2}} \left(\frac{2\sqrt{2}}{\pi}\right)^{\frac{nds}{2n - s}}$$

$$(73) \quad f_2(n, d) = d^{nd + n + s} ((d - 1)!)^{n - s}\, 2^{s \frac{d^2 - 2d - 4}{2}} \left(\frac{2}{\pi}\right)^{\frac{ndr_2}{n - s/2}} \left(\frac{2\sqrt{2}}{\pi}\right)^{\frac{nds}{2n - s}}.$$

Remark 3. Suppose that $B = k$. If $c < 1$, then $\mathrm{Vol}(X(c)) = 2^n d_{\mathcal{D}}$ and Minkowski's theorem would imply that $\mathcal{D} = O_k$ contains a non-zero element with norm to $\mathbb{Z}$ less than 1 in absolute value, which is impossible. Hence $c \geq 1$ and Theorem 5.1 exactly reproduces Lenstra's result.

6. An explicit example

In this section, we compute an explicit example of the bounds in Theorem 4.3. Let B denote the quaternion algebra over $\mathbb{Q}$ ramified exactly at $\{\infty, 2\}$, and let $\mathcal{D}$ be the Hurwitz order

$$\mathbb{Z}\left[I, J, \frac{1+I+J+IJ}{2}\right],$$

where $I^2 = J^2 = -1$. Since $\mathbb{R} \otimes_{\mathbb{Q}} B \cong \mathbb{H}$, we have that the Tamagawa measure on B is $4dx_1 dx_2 dx_3 dx_4$ with respect to the basis $\{1, I, J, IJ\}$, and $d_{\mathcal{D}} = 2$.

Recall that

$$X(c) = \{x \in \mathbb{H} \ : \ |x|_\infty^{d(v)/[k_v:\mathbb{R}]} \leq c\} = \{x \in \mathbb{H} \ : \ |x|_\infty^2 \leq c\},$$

where $|x|_\infty = |\mathrm{N}_\infty(x)|^{1/d(v)}$. Since $d(v) = 2$ and

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

we see that

$$X(c) = \{x = a + bI + cJ + dIJ \in \mathbb{H} \ : \ \|x\| \leq \sqrt{c}\},$$

where $\| \ \|$ is the usual norm on $\mathbb{R}^4$ with respect to the basis $\{1, I, J, IJ\}$. In other words, $X(c)$ is the ball of radius $\sqrt{c}$.

We then see that $X(c)$ has volume

$$4\frac{\pi^2 \sqrt{c}^4}{\Gamma(3)} = 2\pi^2 c^2$$

with respect to the Tamagawa measure on $\mathbb{H}$, where $\Gamma(s)$ is the usual Gamma function. Since we want

$$\mathrm{Vol}(X(c)) \geq 2^{\dim_{\mathbb{Q}}(B)} d_{\mathcal{D}} = 32,$$

we take $c = 4/\pi$. The constant m_X is the largest square-norm of an element of $X(c)$, which is $16/\pi^2$.

6.1. $S = \{\infty\}$. Since $\sqrt{m_X} < 2$, we see that Theorem 4.3 applies to *any* set S containing $\{\infty\}$. That is, the set of finite places that must be in S is empty. In the case $S = \{\infty\}$, we use the above to see that

$$T_2 = T_3' = T_3 = T_4 = 1, \quad T_1 = T_5 = T_6 = 4/\pi.$$

Since $n = 1$ and $d = 2$, plugging these into Theorem 4.3 gives a height bound of $\frac{4}{\pi} < 2$. The height of an element of $\mathcal{D}$ is its reduced norm, so the elements of height less than 2 are those with reduced norm 1. These are the elements of the unit group

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

which is well-known to be the binary tetrahedral group (see Theorem 3.7 of [11]).

6.2. $S = \{\infty\} \cup \{\ell_i\}_{i=1}^h$ for a finite set $\{\ell_i\}_{i=1}^h$ of odd primes. In this section, we prove Theorem 1.2, the statement of which we now recall.

Theorem 6.1. *Let B be Hamilton's quaternion algebra over $\mathbb{Q}$, that is, the rational quaternion algebra with basis $\{1, I, J, IJ\}$ such that $I^2 = J^2 = 1$ and $IJ = -JI$. Let $\mathcal{D}$ be the maximal order*

$$\mathbb{Z}\left[1, I, J, \frac{1 + I + J + IJ}{2}\right]$$

and $S = \{\infty, \ell_1, \ldots, \ell_h\}$ be a set of places containing the archimedean place ∞ and any set $\{\ell_i\}_{i=1}^h$ of distinct odd primes. Then the unit group $\mathcal{D}_S^*$ is generated by the finite set of elements with reduced norm in $\{1, \ell_1, \ldots, \ell_h\}$.

Proof. Let ℓ_h be the largest element of $\{\ell_i\}_{i=1}^h$. Since all the ℓ_i are unramified in B we see that $m_{S_f} = m'_{S_f} = \ell_h$. We can take $T_2 = \ell_h$ and $T_4 = 1$ by (67) and (68), and we can also take $T_3 = T_3' = 1$ and $T_1 = T_5 = 4/\pi$. This gives $T_6 = \ell_h 4/\pi$, and we conclude that $\mathcal{D}^*$ is generated by elements of height bounded by

$$\frac{4}{\pi} \ell_h.$$

We can be more explicit by going back to the statement of Lemma 4.2. Recall that

(74) $\qquad F_X = \{(x, \beta) \in G_S \ : \ x \in X, \ \beta\mathcal{D} \subseteq \mathcal{D}, \ [\mathcal{D} : \beta\mathcal{D}] \leq m_X\}.$

Since $m_X = 16/\pi^2 < 2$, we see that if $(x, \beta) \in F_X$ then $\beta\mathcal{D} = \mathcal{D}$. Thus if ℓ is an element of the set P of topological generators specified in §5.4, and $\gamma \in \Gamma_S \cap (F_X P F_X^{-1})$ as in Lemma 4.2, then for each finite place w there are units $u_w, u_w' \in D_w^*$ such that $\gamma_w = u_w \ell_w (u_w')^{-1}$. Thus $N_w(\gamma)$ equals a unit in O_w^* times $N_w(\ell_w)$ when $N_w : B_w \to k_w$ is the reduced norm. By definition of P, this means that the reduced norm $N(\gamma)$ lies in $\{1, \ell_1, \ldots, \ell_h\}$. Therefore $\Gamma_S = \mathcal{D}_S^*$ is generated by set of $\gamma \in \mathcal{D}$ such that $N(\gamma) \in \{1, \ell_1, \ldots, \ell_h\}$. $\qquad\square$

The fact that the set F_X defined in the proof of Theorem 6.1 is a fundamental domain for the action of $\mathcal{D}_S^*$ on G_S implies the following.

Corollary 6.2. *Let B, $\mathcal{D}$, and S be as in Theorem 6.1. For each $1 \leq i \leq h$, let T_i be the Bruhat–Tits tree associated with $\mathrm{GL}_2(\mathbb{Q}_{\ell_i})$, and set*

$$T = \prod_{i=1}^h T_i.$$

Then the action of $\mathcal{D}_S^*$ on T is vertex transitive. That is, given any pair $(x_1, \ldots, x_h)$ and $(y_1, \ldots, y_h)$, where each x_i and y_i is a vertex of the tree T_i, there exists an element $\gamma \in \mathcal{D}_S^*$ so that $\gamma(x_i) = y_i$ for every $1 \leq i \leq h$.

In comparison, we note that Mohammadi and Salehi Golsefidy [10] classified the maximal discrete subgroups with vertex transitive action on the

Bruhat–Tits building $\mathfrak{B}$ of a simply connected absolutely almost simple k-group over a nonarchimedean field k when $\mathfrak{B}$ has dimension at least 4. In particular, there are finitely many such maximal groups.

Members of the 2012 Arizona winter school on arithmetic geometry used Corollary 6.2 to produce presentations for the groups $\mathcal{D}_S^*$ for various S. See [4]. Unpublished work of Fritz Grunewald computed presentations of $\mathcal{D}_S^1$ for some small S, but to our knowledge, [4] gives the first presentations of groups acting faithfully, irreducibly, and cocompactly on a product of Bruhat–Tits buildings. One such presentation is the following.

Theorem 6.3 ([4]). *With B and $\mathcal{D}$ as above, the group $\mathcal{D}^*_{\{\infty,3,5\}}$ has presentation with generators (the images in $\mathcal{D}^*_{\{\infty,3,5\}}$ of):*

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

and relations:

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

References

[1] BURGER, MARC; SCHROEDER, VIKTOR. Volume, diameter and the first eigenvalue of locally symmetric spaces of rank one. *J. Differential Geom.* **26** (1987), no. 2, 273–284. MR0906391 (89a:53046), Zbl 0599.53042.

[2] CASSELS, J. W. S.; FRÖHLICH, A.; DIRS. Algebraic number theory. *Academic Press, London; Thompson Book Co., Inc., Washington, D.C.* 1967 xviii+366 pp. MR0215665 (35 #6500), Zbl 0153.07403.

[3] CHAN, WAI KIU; FUKSHANSKY, LENNY. Small zeros of Hermitian forms over a quaternion algebra. *Acta Arith.* **142** (2010), no. 3, 251–266. MR2606967 (2011e:11112), Zbl 1209.11060, arXiv:0911.4104, doi:10.4064/aa142-3-3.

[4] CHINBURG, TED; FRIEDLANDER, HOLLEY; HOWE, SEAN; KOSTERS, MICHIEL; SINGH, BHAIRAV; STOVER, MATTHEW; ZHANG, YING; ZIEGLER, PAUL. Presentations for quaternionic S-unit groups. To appear in *Exp. Math.*, 2014. arXiv:1404.6091.

[5] GRUNEWALD, FRITZ; SEGAL, DANIEL. Some general algorithms. I. Arithmetic groups. *Ann. of Math.* (2) **112** (1980), no. 3, 531–583. MR0595206 (82d:20048a), Zbl 0457.20047, doi:10.2307/1971091.

[6] GRUNEWALD, FRITZ; SEGAL, DANIEL. Decision problems concerning S-arithmetic groups. *J. Symbolic Logic* **50** (1985), no. 3, 743–772. MR0805682 (87a:22023), Zbl 0581.20045, doi:10.2307/2274327.

[7] Lenstra, H. W., Jr. Algorithms in algebraic number theory. *Bull. Amer. Math. Soc. (N.S.)* **26** (1992), no. 2, 211–244. MR1129315 (93g:11131), Zbl 0759.11046, arXiv:math/9204234, doi: 10.1090/S0273-0979-1992-00284-7.

[8] Liebendörfer, Christine. Linear equations and heights over division algebras. *J. Number Theory* **105** (2004), no. 1, 101–133. MR2032444 (2005b:11092), Zbl 1055.11042, doi: 10.1016/j.jnt.2003.09.003.

[9] Liebendörfer, Christine. Heights and determinants over quaternion algebras. *Comm. Algebra* **33** (2005), no. 10, 3699–3717. MR2175460 (2006k:11227), Zbl 1082.15014, doi: 10.1080/00927870500243130.

[10] Mohammadi, Amir; Salehi Golsefidy, Alireza. Discrete subgroups acting transitively on vertices of a Bruhat–Tits building. *Duke Math. J.* **161** (2012), no. 3, 483–544. MR2881229, Zbl 1254.22015, doi: 10.1215/00127094-1507430.

[11] Vignéras, Marie-France. Arithmétique des algèbres de quaternions. Lecture Notes in Mathematics, 800. *Springer, Berlin*, 1980. vii+169 pp. ISBN: 3-540-09983-2. MR0580949 (82i:12016), Zbl 0422.12008, doi: 10.1007/BFb0091027.

[12] Weil, André. Basic number theory. Classics in Mathematics. *Springer-Verlag, Berlin*, 1995. xviii+315 pp. ISBN: 3-540-58655-5. MR1344916 (96c:11002), Zbl 0823.11001.

(Ted Chinburg) Department of Mathematics, University of Pennsylvania, 209 South 33rd Street, Philadelphia, PA 10104
`ted@math.upenn.edu`

(Matthew Stover) Department of Mathematics, Temple University, 1805 N. Broad Street, Philadelphia, PA 19122
`mstover@temple.edu`