JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Gebhard BÖCKLE et Ralf BUTENUTH

On computing quaternion quotient graphs for function fields

Tome 24, n° 1 (2012), p. 73-99.

<http://jtnb.cedram.org/item?id=JTNB_2012__24_1_73_0>

Journal de Théorie des Nombres
de Bordeaux **24** (2012), 73-99

On computing quaternion quotient graphs for function fields

par Gebhard BÖCKLE et Ralf BUTENUTH

Résumé. Soit Λ un $\mathbb{F}_q[T]$-ordre maximal d'un corps de quaternions sur $\mathbb{F}_q(T)$ non-ramifié à la place ∞. Cet article donne un algorithme pour calculer un domaine fondamental de l'action du groupe des unités Λ^* sur l'arbre de Bruhat-Tits $\mathcal{T}$ associé à $\mathrm{PGL}_2(\mathbb{F}_q((1/T)))$, l'action étant un analogue en corps de fonctions de l'action d'un groupe cocompact Fuchsian sur le demi-plan supérieur. L'algorithme donne également une présentation explicite du groupe Λ^* par générateurs et relations. En outre nous trouvons une borne supérieure pour le temps de calcul en utilisant que le graphe quotient $\Lambda^*\backslash\mathcal{T}$ est *presque* de Ramanujan.

Abstract. Let Λ be a maximal $\mathbb{F}_q[T]$-order in a division quaternion algebra over $\mathbb{F}_q(T)$ which is split at the place ∞. The present article gives an algorithm to compute a fundamental domain for the action of the group of units Λ^* on the Bruhat-Tits tree $\mathcal{T}$ associated to $\mathrm{PGL}_2(\mathbb{F}_q((1/T)))$. This action is a function field analog of the action of a co-compact Fuchsian group on the upper half plane. The algorithm also yields an explicit presentation of the group Λ^* in terms of generators and relations. Moreover we determine an upper bound for its running time using that $\Lambda^*\backslash\mathcal{T}$ is *almost* Ramanujan.

1. Introduction

A major recent theme in explicit arithmetic geometry over $\mathbb{Q}$ or over more general number fields has been the development and implementation of algorithms to compute automorphic forms [Cr, De, GV, GY, Ste]. More precisely, these algorithms compute the Hecke action on spaces of modular forms for a given level and weight. Typically these algorithms proceed in three steps: (i) a combinatorial or geometric model is provided in which one can compute the Hecke action; (ii) on the model one performs some precomputations such as the computations of ideal classes of a maximal order in a quaternion division algebra, or the computation of a fundamental domain; (iii) on the data provided by (ii) one implements the Hecke action.

Manuscrit reçu le 22 octobre 2010.

The present article is concerned with an analogous algorithm over function fields whose ultimate goal is the computation of Drinfeld modular forms as well as automorphic forms. For GL_2 over function fields, (i) and (ii) were solved in [Te1] and [Te2, GN], respectively. Here we will be concerned with inner forms of GL_2 that correspond to the unit group of a quaternion division algebra split at ∞. In this setting an extension of [Te1] is part of [Bu]. The sought-for combinatorial description of the forms to be computed is given in terms of harmonic cocycles on the Bruhat-Tits tree which are invariant under the action of an arithmetic subgroup Γ defined from the division algebra. The main precomputation that makes up step (ii) is that of a fundamental domain of $\mathcal{T}$ under the action of Γ. This can be thought of as an analog of [Vo]. Due to the different underlying *geometry* the methods employed are completely different.

To describe the output of our algorithm and some consequences note first that in our setting of a quaternion division algebra split at ∞, the quotient $\Gamma\backslash\mathcal{T}$ is a finite graph. The fundamental domain with an edge pairing that we compute consists of the following data:

(1) a finite subtree $Y \subset \mathcal{T}$ whose image $\overline{Y}$ in $\Gamma\backslash\mathcal{T}$ is a maximal spanning tree, i.e., $\overline{Y}$ is a tree such that adding any edge of $\Gamma\backslash\mathcal{T}$ to it will create a cycle.
(2) for any edge $\bar{e}$ of $(\Gamma\backslash\mathcal{T}) \setminus \overline{Y}$, an edge e of $\mathcal{T}$ connected to Y that maps to $\bar{e}$ and a the gluing datum that connects the loose vertex of this edge via the action of Γ to a vertex of Y.

What we compute is the analog of fundamental domain together with a side pairing in the sense of [Vo]. As explained in [Se1, § I.4], this data yields a presentation of the group Γ in terms of explicit generators and relations. Moreover the fundamental domain data computed provides an efficient reduction algorithm on the tree: to any edge it computes its representative in Y', by which we mean the union of Y with the edges in (2). Reinterpreted in terms of group theory, a fundamental domain with an edge pairing yields an efficient algorithm to solve the word problem for Γ.

Observing that a finite cover of $\Gamma\backslash\mathcal{T}$ is a Ramanujan graph, yields a bound on the diameter of $\Gamma\backslash\mathcal{T}$. This in turn we use to bound the complexity of our algorithm, to bound the size of Y', and to bound the size of the representatives of Y' in terms of a natural height on the 2×2-matrices over the function field completed at ∞. Our main result is therefore the existence of an effective algorithm together with precise complexity bounds. An implementation can be obtained on request from the second author.

A theoretical result on the size of a minimal generating set for Γ and the (logarithmic) height of its generators was obtained by different methods in [Pa2]. Our height bound is better by a factor of 2. The results in [Pa2] also prove the existence of an algorithm to compute a fundamental domain. An

implementation or a detailed analysis of that algorithm have not yet been carried out. Both [Pa2] and the present article rely heavily on [Pa1].

We conclude by a short overview of the article: in Sections 2, 3 and 4, we recall basic notions and results from graph theory, on the Bruhat-Tits tree and from the theory of quaternion algebras. Section 5 introduces the main object of this article, the action of Γ on the Bruhat-Tits tree $\mathcal{T}$, and states relevant results on the resulting quotient graph $\Gamma\backslash\mathcal{T}$. Our basic algorithm is presented in Section 6, except that we use one unproved subroutine which is the content of the following Section 7. The algorithm can be viewed as a local (function field) variant of the neighborhood method by Kneser at one place. The final Sections 8 and 9 present on the one hand the applications of the algorithm to the presentation of Γ in terms of generators and relations and to the word problem, and on the other hand the complexity analysis of the algorithm based on the fact that $\Gamma\backslash\mathcal{T}$ has a finite cover that is Ramanujan.

Acknowledgments: For several useful discussions we wish to thank Mihran Papikian and John Voight. We also want to heartily thank the anonymous referee whose many comments and suggestions greatly improved the readability of the present article. During this work, the authors were supported by the Sonderforschungsbereich/Transregio 45 *Periods, Moduli Spaces and Arithmetic of Algebraic Varieties* and by the DFG priority project SPP 1489. The implementation of the algorithm is based on the computer algebra system Magma [BCP].

Notation. Throughout this article $K = \mathbb{F}_q(T)$ will denote the rational function field over $\mathbb{F}_q$. As usual, the infinite valuation v_∞ on K is defined by $v_\infty(\frac{f}{g}) = \deg(g) - \deg(f)$ for $f, g \in A = \mathbb{F}_q[T], g \neq 0$ and $v_\infty(0) = \infty$. Then $\pi = 1/T$ is a uniformizer for v_∞, the corresponding completion of K is $K_\infty = \mathbb{F}_q((\pi))$ and we write $\mathcal{O}_\infty$ for its ring of integers.

Remark. The restriction that q be odd is for the sake of simplicity of exposition. To treat the case that q is even, one needs to redo all of Section 4 with very little overlap with the odd case. Some changes are also necessary in Section 7. All other results hold independently of q being even or odd. We have implemented our algorithm also for even q. More details on the case of even q can be found in [Bu].

2. Notions from graph theory

Definition 2.1. A *(directed multi-)graph* $\mathcal{G}$ is a pair $(\mathrm{V}(\mathcal{G}), \mathrm{E}(\mathcal{G}))$ where $\mathrm{V}(\mathcal{G})$ is a (possibly infinite) set and $\mathrm{E}(\mathcal{G})$ is a subset of $\mathrm{V}(\mathcal{G}) \times \mathrm{V}(\mathcal{G}) \times \mathbb{Z}_{\geq 0}$ such that

(1) for any $(v, v') \in \mathrm{V}(\mathcal{G}) \times \mathrm{V}(\mathcal{G})$, the set $\{i \in \mathbb{Z}_{\geq 0} \mid (v, v', i) \in \mathrm{E}(\mathcal{G})\}$ is a finite initial segment of $\mathbb{Z}_{\geq 0}$ of cardinality denoted by $n_{v,v'}$,

(2) for $e = (v, v', i) \in \mathrm{E}(\mathcal{G})$ its opposite $e^\star = (v', v, i)$ lies in $\mathrm{E}(\mathcal{G})$,
(3) for any $v \in \mathrm{V}(\mathcal{G})$, the set $\mathrm{Nbs}(v) := \{v' \in \mathrm{V}(\mathcal{G}) \mid (v, v', 0) \in \mathrm{E}(\mathcal{G})\}$ is finite.

An element $v \in \mathrm{V}(\mathcal{G})$ is called a *vertex*, an element $e \in \mathrm{E}(\mathcal{G})$ is called an *(oriented) edge* and an element in $\mathrm{V}(\mathcal{G}) \sqcup \mathrm{E}(\mathcal{G})$ is called a *simplex*. For each edge $e = (v, v', i) \in \mathrm{E}(\mathcal{G})$ we call $o(e) := v$ the *origin* of e and $t(e) := v'$ the *target* of e. If there is only one edge between vertices v, v' of $\mathcal{G}$ we simply write (v, v') instead of $(v, v', 0)$. Two vertices v, v' are called *adjacent*, if $\{v, v'\} = \{o(e), t(e)\}$ for some edge e. An edge e with $o(e) = t(e)$ is called a *loop*. A vertex v is called terminal if there is only one edge e with $o(e) = v$.

Let $v, v' \in \mathrm{V}(\mathcal{G})$. A *path* from v to v' is a finite sequence $(e_1, \ldots, e_k)$ in $\mathrm{E}(\mathcal{G})$ such that $t(e_i) = o(e_{i+1})$ for all $i = 1, \ldots, k-1$ and $o(e_1) = v$, $t(e_k) = v'$. The integer k is called the *length* of the path $(e_1, \ldots, e_k)$. The *distance* from v to v', denoted $d(v, v')$, is the minimal length among all paths from v to v' (or ∞ if no such path exists). A path $(e_1, \ldots, e_k)$ from v to v' without backtracking, i.e., such that for no i we have $e_i = e_{i-1}^\star$, is called a *geodesic*. Note that the length of a geodesic need not be $d(v, v')$ but that $d(v, v')$ is attained for a geodesic.

A graph $\mathcal{G}$ is *connected* if for any two vertices $v, v' \in \mathrm{V}(\mathcal{G})$ there is a path from v to v'. A *cycle* of $\mathcal{G}$ is a geodesic from some vertex v to itself. Therefore a loop is a cycle of length one. A graph $\mathcal{G}$ is *cycle-free* if it contains no cycles. A *tree* is a connected, cycle-free graph. If $\mathcal{G}$ is a tree, then any two vertices of $\mathcal{G}$ are connected by a unique geodesic.

A *subgraph* $\mathcal{G}' \subseteq \mathcal{G}$ is a graph $\mathcal{G}'$ such that $\mathrm{V}(\mathcal{G}') \subseteq \mathrm{V}(\mathcal{G})$ and $\mathrm{E}(\mathcal{G}') \subseteq \mathrm{E}(\mathcal{G})$. Any subgraph $\mathcal{S} \subseteq \mathcal{G}$ which is a tree is called *subtree*. A *maximal subtree* is a subtree which is maximal under inclusion among all subtrees of $\mathcal{G}$.

The *degree* of $v \in \mathrm{V}(\mathcal{G})$ is

$$\deg(v) := \deg_{\mathcal{G}}(v) := \#\{e \in \mathrm{E}(\mathcal{G}) \mid o(e) = v\}.$$

A graph $\mathcal{G}$ is called *k-regular* if for all vertices $v \in \mathrm{V}(\mathcal{G})$ we have $\deg(v) = k$.

A graph $\mathcal{G}$ is *finite*, if $\#\,\mathrm{V}(\mathcal{G}) < \infty$. Then also $\#\,\mathrm{E}(\mathcal{G}) < \infty$, since $\deg(v)$ is finite for all $v \in \mathrm{V}(\mathcal{G})$. The *diameter* of a (finite) graph $\mathcal{G}$ is

$$\mathrm{diam}(\mathcal{G}) := \max_{v, v' \in \mathrm{V}(G)} d(v, v').$$

Definition 2.2. The *first Betti number* $h_1(\mathcal{G})$ of a finite connected graph is

$$h_1(\mathcal{G}) := \frac{\#\,\mathrm{E}(\mathcal{G})}{2} - \#\,\mathrm{V}(\mathcal{G}) + 1.$$

A graph $\mathcal{G}$ defines an abstract simplicial set. Its geometric realization is a topological space $|\mathcal{G}|$. For finite graphs one has $h_1(\mathcal{G}) = \dim_{\mathbb{Q}} H_1(|\mathcal{G}|, \mathbb{Q})$, i.e., the Betti number counts the number of independent cycles of $\mathcal{G}$.

3. The Bruhat-Tits tree

In this section, we recall the definition of the Bruhat-Tits tree for the group $\mathrm{PGL}_2(K_\infty)$. It is an important combinatorial object for the arithmetic of K. The material can be found in [Se1].

One defines a graph $(\mathrm{V}(\mathcal{T}), \mathrm{E}(\mathcal{T}))$ as follows: Two $\mathcal{O}_\infty$-lattices $L, L' \subset K_\infty^2$ are called equivalent if there is a $\lambda \in K_\infty^*$ with $L' = \lambda L$. The set $\mathrm{V}(\mathcal{T})$ is the set of equivalence classes $[L]$ of such lattices. The set $\mathrm{E}(\mathcal{T})$ is the set of pairs $([L], [L'])$ such that $L, L' \subset K_\infty^*$ are $\mathcal{O}_\infty$-lattices with $\pi L \subsetneq L' \subsetneq L$, or equivalently such that $L' \subsetneq L$ and $L/L' \cong \mathbb{F}_q$ as $\mathcal{O}_\infty$-modules. In particular there is at most one edge between any two vertices.

By [Se1, § II.1] the graph $\mathcal{T} = (\mathrm{V}(\mathcal{T}), \mathrm{E}(\mathcal{T}))$ is a $q+1$-regular tree – recall that q is the cardinality of the residue field of K_∞. The group $\mathrm{PGL}_2(K_\infty)$ acts naturally on lattice classes by left multiplication $(g, [L]) \mapsto [gL]$. This induces an action on $\mathcal{T}$. Because the definitions are a special case of a general construction, one calls $\mathcal{T}$ the *Bruhat-Tits tree for* $\mathrm{PGL}_2(K_\infty)$.

Let $e_1 = (1,0)^t$ and $e_2 = (0,1)^t$ be the standard basis of K_∞^2, thought of as column vectors. Write $\mathcal{O}_\infty^2$ for $\mathcal{O}_\infty e_1 \oplus \mathcal{O}_\infty e_2$. The following result is well-known and straightforward, using the class equation and the transitive action of $\mathrm{GL}_2(K_\infty)$ on bases of K_∞^2.

Proposition 3.1. *The map*

$$\begin{array}{rcl} \phi : \mathrm{GL}_2(K_\infty)/\mathrm{GL}_2(\mathcal{O}_\infty)K_\infty^* & \to & \mathrm{V}(\mathcal{T}) \\ A & \mapsto & \left[A\mathcal{O}_\infty^2\right] \end{array}$$

is a bijection of left $\mathrm{GL}_2(K_\infty)$*-sets.*

The map ϕ of the above proposition allows us to represent vertices of $\mathcal{T}$ by elements of $\mathrm{GL}_2(K_\infty)$. Row-reduction to the echelon form of a matrix yields a standard representative in $\mathrm{GL}_2(K_\infty)$ as expressed by the following result.

Lemma 3.2. *Every class of* $\mathrm{GL}_2(K_\infty)/\mathrm{GL}_2(\mathcal{O}_\infty)K_\infty^*$ *has a unique representative of the form*

$$\begin{pmatrix} \pi^n & g \\ 0 & 1 \end{pmatrix}$$

with $n \in \mathbb{Z}$ *and* $g \in K_\infty/\pi^n\mathcal{O}_\infty$*, called its* vertex normal form.

We also need a criterion for adjacency for matrices in vertex normal form.

Lemma 3.3. *Consider the two matrices in vertex normal form*

$$A := \begin{pmatrix} \pi^n & g \\ 0 & 1 \end{pmatrix}, B := \begin{pmatrix} \pi^{n+1} & g + \alpha\pi^n \\ 0 & 1 \end{pmatrix}$$

with $n \in \mathbb{Z}, \alpha \in \mathbb{F}_q, g \in K_\infty/\pi^n\mathcal{O}_\infty$ and let L_1 and L_2 be the two lattices

$$L_1 := A\mathcal{O}_\infty^2, L_2 := B\mathcal{O}_\infty^2.$$

Then $L_1 \supset L_2$ and $L_1/L_2 \cong \mathbb{F}_q$.

Remark 3.4. Lemma 3.3 only displays q vertices adjacent to $[L_1]$. The missing one is the class of $\begin{pmatrix} \pi^{n-1} & g \\ 0 & 1 \end{pmatrix} \mathcal{O}_\infty^2$ with g now being replaced by its class in $K_\infty/\pi^{n-1}\mathcal{O}_\infty$.

Figure 3.1 below illustrates the tree together with the matrices in normal form corresponding to vertices. The identification is clear from the previous lemma. Note that each line in the picture symbolizes a whole fan expanding to the right. The elements $\alpha \in \mathbb{F}_q^*$, $\beta \in \mathbb{F}_q$ agree on each fan.

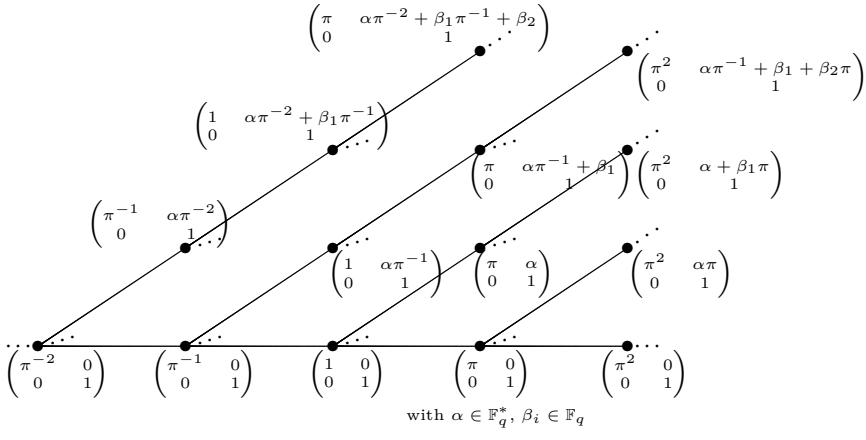

FIGURE 3.1. The tree $\mathcal{T}$ with the corresponding matrices

Write $L(n,g)$ for the $\mathcal{O}_\infty$-lattice $\langle v_1, v_2\rangle_{\mathcal{O}_\infty}$ where $v_1 = \begin{pmatrix} \pi^n \\ 0 \end{pmatrix}$ and $v_2 = \begin{pmatrix} g \\ 1 \end{pmatrix}$. Note that $L(n,g) = L(n,g')$ if and only if $g \equiv g' \pmod{\pi^n\mathcal{O}_\infty}$.

Remark 3.5. For $n \in \mathbb{Z}$, $g \in K_\infty$ we define

$$\delta := \deg_n(g) := \min\{i \in \mathbb{Z}_{\geq 0} \mid g \in \pi^{n-i}\mathcal{O}_\infty\}.$$

Then the path from $L(n,g)$ to $L(0,0)$ in $\mathcal{T}$ is

$$L(n,g) \text{ —— } L(n-1,g) \text{ —— } \ldots \text{ —— } L(n-\delta,g) = L(n-\delta,0) \text{ —}$$
$$\text{—— } L(\mathrm{sgn}(n-\delta)\cdot(|n-\delta|-1),0) \text{ —— } \ldots \text{ —— } L(\mathrm{sgn}(n-\delta)\cdot 1,0) \text{ —— } L(0,0)$$

In particular the distance between $L(n,g)$ and $L(0,0)$ is $\deg_n(g) + |n - \deg_n(g)|$.

4. Quaternion algebras

We recall standard facts on quaternion algebras over $K = \mathbb{F}_q(T)$ and over completions of K, and on orders over $A = \mathbb{F}_q[T]$. We assume throughout that q is odd. Our basic references are [JS, Kap. IX] and [Vi]. Many results stated are true more generally. However, we confine ourselves to the case at hand.

A quaternion algebra over a field F is a central simple algebra of dimension 4 over F. It is either isomorphic to $M_2(F)$ or a division algebra. One has the following well-known construction of quaternion algebras.

Construction 4.1. *For $a, b \in F^*$ one defines $\left(\frac{a,b}{F}\right)$ as the K-algebra with F-basis $1, i, j, ij$ and relations $i^2 = a, j^2 = b, ij = -ji$.*

The relations can be expanded to a 4×4 multiplication table for the given F-basis of $\left(\frac{a,b}{F}\right)$. One shows that $\left(\frac{a,b}{F}\right)$ defines a quaternion algebra over F, and that conversely any quaternion algebra over F can be obtained via this construction for a suitable choice of $a, b \in F^*$.

Among other things, a quaternion algebra D over F carries a *reduced norm map* $\mathrm{nrd}\colon D \to F$ which defines a quadratic form on D. For $D = \left(\frac{a,b}{F}\right)$ the reduced norm has the explicit expression

$$\mathrm{nrd}(\gamma) = \gamma_1^2 - a\gamma_2^2 - b\gamma_3^2 + ab\gamma_4^2$$

for any $\gamma = \gamma_1 + \gamma_2 i + \gamma_3 j + \gamma_4 ij \in D$ with $(\gamma_1, \gamma_2, \gamma_3, \gamma_4) \in F^4$. If D is isomorphic to $M_2(F)$, then nrd is simple the determinant map $\det\colon M_2(F) \to F$.

Let now D denote a quaternion algebra over K. Then $D_{\mathfrak{p}} := D \otimes_K K_{\mathfrak{p}}$ is a quaternion algebra over the completion $K_{\mathfrak{p}}$ for any place $\mathfrak{p}$ of K.

Definition 4.2. D is *ramified* at $\mathfrak{p}$ if and only if $D_{\mathfrak{p}}$ is a division algebra.

Definition 4.3. The *Hilbert symbol* of a pair $(a, b) \in K^2$ at a place $\mathfrak{p}$ is

$$(a,b)_{K_{\mathfrak{p}}} := \begin{cases} +1 & \left(\frac{a,b}{K}\right) \text{ is unramified at } \mathfrak{p} \\ -1 & \left(\frac{a,b}{K}\right) \text{ is ramified at } \mathfrak{p}. \end{cases}$$

Definition 4.4. For $a \in A$ and ϖ an irreducible element of A, the *Legendre symbol of a at ϖ* is

$$\left(\frac{a}{\varpi}\right) := \begin{cases} 1 & a \notin \varpi A \text{ and } a \text{ is a square modulo } \varpi \\ -1 & a \text{ is a non-square modulo } \varpi \\ 0 & a \in \varpi A. \end{cases}$$

By adaptating to the function-field situation the proof of [Se2, Ch. III, Thm. 1], the following result is straightforward.

Proposition 4.5. *Suppose q is odd. Write $\mathfrak{p} = (\varpi)$ and let $a = \varpi^\alpha u, b = \varpi^\beta v$ with $u, v \in O_{K_\mathfrak{p}}^*, \alpha, \beta \in \mathbb{Z}$ and let $\epsilon(\mathfrak{p}) := \frac{q-1}{2} \deg(\varpi) \pmod 2$. Then*

$$(a,b)_{K_\mathfrak{p}} = (-1)^{\alpha\beta\epsilon(\mathfrak{p})} \left(\frac{u}{\varpi}\right)^\beta \left(\frac{v}{\varpi}\right)^\alpha.$$

Let R denote the set of all ramified places of D. Then [Vi, Lem. III.3.1 and Thme. III.3.1] yields the following.

Proposition 4.6. *The cardinality of R is finite and even and D is up to isomorphism uniquely determined by R. The set R is empty if and only if $D \cong M_2(K)$.*

The ideal $\mathfrak{r} := \prod_{\mathfrak{p}\in R} \mathfrak{p}$ of A is called the *discriminant* of D. Let $r \in A$ be the monic generator of $\mathfrak{r}$.

Assumption 4.7. *For the remainder of this article, we assume that D is a division quaternion algebra which is unramified at ∞, i.e., that D is an indefinite quaternion algebra over A. We also fix an isomorphism $D_\infty \cong M_2(K_\infty)$.*

Let Λ be an order of D over A. It is free over A of rank 4 and so we may choose a basis $f_1, \ldots, f_4$. The ideal generated by

$$\operatorname{disc}(f_1, \ldots, f_4) := \det(\operatorname{trd}(f_i f_j))_{i,j=1,\ldots,4}$$

is independent of the chosen basis. By [Vi, Lem. I.4.7], this ideal is a square and one defines the *reduced discriminant* $\operatorname{rdisc}(\Lambda)$ of Λ as the square root of this ideal. One deduces a criterion for an order to be maximal, see [Vi, Cor. III.5.3].

Proposition 4.8. *An A-order Λ is maximal in D if and only if* $\operatorname{rdisc}(\Lambda) = \mathfrak{r}$.

Since D is split at infinity and K has class number 1, [Vi, Cor. III.5.7] yields:

Proposition 4.9. *All maximal A-orders Λ in D are conjugate under D^*.*

Let $\Gamma := \Lambda^*$ be the group of units of of a maximal order Λ. By what we have said so far, Γ depends uniquely up to conjugation on D, i.e., on K and R.

From global to local compatibilities and explicit local results, one deduces the following assertions.

Lemma 4.10. (1) *The reduced norm* nrd *maps Λ to A.*
(2) $\Gamma = \{\gamma \in \Lambda \mid \operatorname{nrd}(\gamma) \in \mathbb{F}_q^*\}$.

(3) *The embedding* $\iota: D \hookrightarrow D_\infty \cong M_2(K_\infty)$ *restricts to a group monomorphism*

$$\Gamma \longhookrightarrow \mathrm{SL}_2(K_\infty) \begin{pmatrix} \mathbb{F}_q^* & 0 \\ 0 & 1 \end{pmatrix} \subset \mathrm{GL}_2(K_\infty).$$

The following result is well-known. In lack of an explicit reference, we shall give a proof.

Proposition 4.11. *Via* ι *the group* Γ *is a discrete subgroup of* $\mathrm{GL}_2(K_\infty)$.

Proof. The open sets $\{1 + \pi^n M_2(\mathcal{O}_\infty) \mid n \in \mathbb{N}\}$ form a basis of open neighborhoods of 1 in $\mathrm{GL}_2(K_\infty)$. After shifting by 1 it suffices to show that $\Lambda \cap M_2(\mathcal{O}_\infty)$ is finite, or in other words that Λ is discrete in $M_2(K_\infty)$.

To see the discreteness, let $\mathcal{D}$ be the unique locally free coherent sheaf of rings of rank 4 over $\mathbb{P}^1_{\mathbb{F}_q}$ such that $\Lambda \cong \Gamma(\mathbb{A}^1_{\mathbb{F}_q}, \mathcal{D})$ and such that the completed stalk at infinity satisfies $\mathcal{D}_\infty \cong M_2(\mathcal{O}_\infty)$. Then $\Lambda \cap M_2(\mathcal{O}_\infty) = H^0(\mathbb{P}^1_{\mathbb{F}_q}, \mathcal{D})$. By the Riemann-Roch Theorem, this is a finite-dimensional $\mathbb{F}_q$-vector space.

Alternatively, for D and Λ constructed later in Propositions 4.15 and 4.16, and the embedding from Lemma 4.17, the discreteness can be verified explicitly, by proving that an A-Basis of Λ maps to a K_∞-basis of D_∞. □

Given an even set R of finite places of K at which D is ramified, the algorithm described in Sections 6 and 7 will be based on a concrete model for (D, Λ). In the remainder of this section we describe such a model. It will consist of an explicit pair $(a, b) \in K^*$ such that $D \cong \left(\frac{a,b}{K}\right)$ and an explicit basis of a maximal A-order Λ of $\left(\frac{a,b}{K}\right)$.

Let $l \geq 2$ be even and let R be a set of l-distinct prime ideals $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_l\}$ of A. Denote by ϖ_i the unique monic (irreducible) generator of $\mathfrak{p}_i$. Set $r := \prod_i \varpi_i$ and $\mathfrak{r} := \prod_i \mathfrak{p}_i$ where the index i ranges over $1, \ldots, l$.

Lemma 4.12. *There is an irreducible monic polynomial* $\alpha \in A$ *of even degree such that*

$$\left(\frac{\alpha}{\varpi_i}\right) = -1 \text{ for all } i. \tag{4.1}$$

Any such α *also satisfies* $\left(\frac{r}{\alpha}\right) = 1$.

Proof. Choose any $a \in A$ such that

$$\left(\frac{a}{\varpi_i}\right) = -1$$

for all i. This can be done using the Chinese remainder theorem. By the strong form of the function field analogue of Dirichlet's theorem on primes in arithmetic progression, [Ro, Thm. 4.8], the set $\{a + rb \mid b \in A\}$ contains

an irreducible monic polynomial α of even degree. Since $\alpha \equiv a \pmod{\varpi_i}$ we have

$$\left(\frac{\alpha}{\varpi_i}\right) = -1$$

for all i. By quadratic reciprocity, [Ro, Thm. 3.3], we deduce

$$\left(\frac{\varpi_i}{\alpha}\right) = (-1)^{\frac{q-1}{2}\deg\alpha\deg\varpi_i}\left(\frac{\alpha}{\varpi_i}\right) = -1$$

since $\deg(\alpha)$ is even. But then because l is even, we find

$$\left(\frac{r}{\alpha}\right) = \prod_{i=1}^{l}\left(\frac{\varpi_i}{\alpha}\right) = (-1)^l = 1.$$

□

Remark 4.13. In practice α is rapidly found by the following simple search:

Step 1: Start with $m = 2$.
Step 2: Check for all monic irreducible $\alpha \in A$ of degree m whether $\left(\frac{\alpha}{\varpi_i}\right) = -1$ for all $1 \le i \le l$.
Step 3: If we found an α then stop. Else increase m by 2 and go back to Step 2.

In the function field setting [MS] gives an unconditional effective version of the Čebotarov density theorem. This allows us to make Lemma 4.12 effective, i.e., to give explicit bounds on $\deg(\alpha)$ in terms of $\deg(r)$.

Proposition 4.14. *Abbreviate $d := \deg(r)$. The following table gives upper bounds on $d_\alpha := \deg(\alpha)$ depending on q and l:*

	$q=3$			$q=5,7$		$q=9$		$q \ge 11$	
	$l \le 4$	$l=6$	$8 \le l$	$l \le 6$	$8 \le l$	$l \le 4$	$6 \le l$	$l=2$	$4 \le l$
$d_\alpha \le$	$d+7$	$d+5$	$d+1$	$d+3$	$d+1$	$d+3$	$d+1$	$d+3$	$d+1$

A basic reference for the results on function fields used in the following proof is [Sti].

Proof. Let $K' := K(\sqrt{\varpi_1}, \ldots, \sqrt{\varpi_l})$. Then K'/K is a Galois extension with Galois group isomorphic to $\{\pm 1\}^l$ with $\{\pm 1\} \cong \mathbb{Z}/(2)$; its branch locus in K is the divisor $\mathcal{D}$ consisting of the sum of the (ϖ_k) and (possibly) ∞; the constant field of K' is again $\mathbb{F}_q$. Denote by g' the genus of K' and by $\mathcal{D}'$ the ramification divisor of K'/K. The ramification degree at all places is 1 or 2 and hence tame because q is odd. It follows that $\deg(\mathcal{D}') = \#G/2 \cdot \deg(\mathcal{D})$.

Let $\pi(k)$ denote the places of K of degree k; let $\pi_C(k)$ denote the places $\mathfrak{p}$ of K of degree k for which $\mathrm{Frob}_\mathfrak{p} = (-1, \ldots, -1) \in \{\pm 1\}^l$. Note that the elements of $\pi_C(k)$ are in bijection to the monic irreducible polynomials α of

degree k which satisfy the conditions (4.1). The following two inequalities are from [MS, Thm. 1 and (1.1)] and the Hurwitz formula, respectively:

$$|\pi_C(k) - \frac{1}{\#G}\pi(k)| \le 2g' \frac{1}{\#G}\frac{q^{k/2}}{k} + 2\frac{q^{k/2}}{k} + (1+\frac{1}{k})\deg(\mathcal{D}'). \tag{4.2}$$

$$|q^k + 1 - k\pi(k)| \le 2g' \frac{q^{k/2}}{k}. \tag{4.3}$$

$$2g' = -2\#G + \deg(\mathcal{D}') + 2. \tag{4.4}$$

After some manipulations one obtains

$$\pi_C(k) \ge \frac{1}{\#G}\frac{q^k+1}{k} - \frac{q^{k/2}}{k}(\frac{\deg(\mathcal{D})}{2} + 2 + \frac{2}{\#G}) - (1+\frac{1}{k})\#G\frac{\deg(\mathcal{D})}{2}.$$

To ensure that the right hand side is positive for some (even) k, it thus suffices that

$$f(k) := q^k - q^{k/2}\Big(2^{l-1}(\deg(r)+5)+2\Big) - (k+1)2^{2l-1}(\deg(r)+1) > 0. \tag{4.5}$$

We know that l is the number of prime factors of r and hence that $l \le \deg(r)$. There are at most q places of degree 1 and so for small q such as $3, 5, 7$, already for small l the degree of r must be quite a bit larger than l. For instance if $l \ge 7$ and $q = 3$, then $\deg(r) \ge 3l - 9$. Using these considerations and simple analysis on $f(k)$, it is simple if tedious to obtain the lower bounds in the table. We leave details to the reader. □

Proposition 4.15. *For α as in Lemma 4.12, the quaternion algebra $D := (\frac{\alpha, r}{K})$ is ramified exactly at R.*

Proof. The proof is an immediate consequence of Proposition 4.5. □

Since r is a square modulo α, there are $\epsilon, \nu \in A$ with $\deg(\epsilon) < \deg(\alpha)$ and $\epsilon^2 = r + \nu\alpha$.

Proposition 4.16. $\Lambda := A + Ai + Aj + A\frac{\epsilon i + ij}{\alpha}$ *is a maximal A-order of D.*

Proof. This follows easily from Proposition 4.8 by computing the reduced discriminant of the A-basis given. □

Since α has even degree and is monic, there exists a square root of α in K_∞. We choose one and denote it by $\sqrt{\alpha}$. The following result provides an explicit realization for the embedding in Lemma 4.10(c).

Lemma 4.17. *The K-algebra homomorphism $\iota : D \to M_2(K_\infty)$ defined by $i \mapsto \begin{pmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{pmatrix}$ and $j \mapsto \begin{pmatrix} 0 & 1 \\ r & 0 \end{pmatrix}$ induces an isomorphism $D \otimes_K K_\infty \cong M_2(K_\infty)$.*

Proof. One verifies $\iota(i)^2 = \alpha, \iota(j)^2 = r$ and $\iota(i)\iota(j) = -\iota(j)\iota(i)$ by an explicit calculation. □

5. Facts about quaternion quotient graphs

In Section 3 we have described the natural action of $\mathrm{GL}_2(K_\infty)$ on the Bruhat-Tits tree $\mathcal{T}$. In the previous section, starting from D as in Assumption 4.7, we have produced a discrete subgroup $\Gamma \subset \mathrm{GL}_2(K_\infty)$, the unit group of a maximal order. In this section we gather some known results about the induced action of Γ on $\mathcal{T}$ and the quotient graph $\Gamma\backslash\mathcal{T}$. We mainly follow [Pa1].

Lemma 5.1 ([Se1, Cor. to Prop II.1])**.** *For $v \in \mathrm{V}(\mathcal{T})$ and $\gamma \in \Gamma$, the distance $d(v, \gamma v)$ is even.*

Proposition 5.2 ([Pa1, Lem. 5.1])**.** *The graph $\Gamma\backslash\mathcal{T}$ is finite graph.*

Proposition 5.3 ([Pa1, Prop. 5.2])**.** *Let $v \in \mathrm{V}(\mathcal{T})$ and $e \in \mathrm{E}(\mathcal{T})$. Then $\Gamma_v := \mathrm{Stab}_\Gamma(v)$ is either isomorphic to $\mathbb{F}_q^*$ or $\mathbb{F}_{q^2}^*$. $\Gamma_e := \mathrm{Stab}_\Gamma(e)$ is isomorphic to $\mathbb{F}_q^*$.*

Note that the scalar matrices with diagonal in $\mathbb{F}_q^*$ are precisely the scalar matrices in Γ. Clearly they act trivially on $\mathcal{T}$. Hence a stabilizer of a simplex is isomorphic to $\mathbb{F}_q^*$ precisely if it is the set of scalar matrices with diagonal in $\mathbb{F}_q^*$.

We define $\bar{\Gamma}$ to be the image of Γ in $\mathrm{PGL}_2(K_\infty)$ – after what we have just said we have $\bar{\Gamma} \cong \Gamma/\mathbb{F}_q^*$. Then $\bar{\Gamma}_v := \mathrm{Stab}_{\bar{\Gamma}}(v)$ is either trivial or isomorphic to $\mathbb{F}_{q^2}^*/\mathbb{F}_q^* \cong \mathbb{Z}/(q+1)$ and $\bar{\Gamma}_e := \mathrm{Stab}_{\bar{\Gamma}}(e)$ is always trivial.

Definition 5.4 ([Se1, II.2.9])**.** We call a simplex t *projectively stable* if $\bar{\Gamma}_t$ is trivial and *projectively unstable* otherwise.

Corollary 5.5. *Let $v \in \mathrm{V}(\mathcal{T})$ be projectively unstable. Then Γ_v acts transitively on the vertices adjacent to v.*

Let

$$\mathrm{odd}(R) := \begin{cases} 0 & \text{if some place in } R \text{ has even degree,} \\ 1 & \text{otherwise} \end{cases}$$

and let

$$g(R) := 1 + \frac{1}{q^2-1}\left(\prod_{\mathfrak{p}\in R}(q_\mathfrak{p}-1)\right) - \frac{q}{q+1}2^{\#R-1}\,\mathrm{odd}(R)$$

where $q_\mathfrak{p} = q^{\deg(\mathfrak{p})}$. Let $\pi : \mathcal{T} \to \Gamma\backslash\mathcal{T}$ be the natural projection.

Theorem 5.6 ([Pa1, Thm. 5.5])**.** (1) *The graph $\Gamma\backslash\mathcal{T}$ has no loops.*

(2) $h_1(\Gamma\backslash\mathcal{T}) = g(R)$.

(3) *For $\bar{v} \in \Gamma\backslash\mathcal{T}$ and $v \in \pi^{-1}(\bar{v})$ we have:*

- (a) *v is projectively stable if and only if $\bar{v}$ has degree $q+1$.*
- (b) *v is projectively unstable if and only if $\bar{v}$ is terminal.*

(4) *Let V_1 (resp. V_{q+1}) be the number of terminal (resp. degree $q+1$) vertices of $\Gamma\backslash\mathcal{T}$. Then*

$$V_1 = 2^{\#R-1}\,\mathrm{odd}(R) \text{ and } V_{q+1} = \frac{1}{q-1}(2g(R) - 2 + V_1).$$

6. An algorithm to compute a fundamental domain

Let the notation $\mathcal{T}$, Γ be as in the previous section.

Definition 6.1 ([Se1, § I.3])**.** Let G be a group acting on a graph $\mathcal{X}$. A *tree of representatives of* $\mathcal{X}$ (mod G) is a subtree $\mathcal{S} \subset \mathcal{G}$ whose image in $G\backslash\mathcal{X}$ is a maximal subtree.

The following definition is basically [Se1, § I.4.1, Lem. 4], see also [Se1, § I.5.4, Thm. 13]. Note that (a) differs from [Se1, § I.4.1, Def. 7].

Definition 6.2. Let G be a group acting on a tree $\mathcal{X}$.

(1) A *fundamental domain for $\mathcal{X}$ under G* is a pair $(\mathcal{S}, \mathcal{Y})$ of subgraphs $\mathcal{S} \subset \mathcal{Y} \subset \mathcal{X}$ such that
   (a) $\mathcal{S}$ is a tree of representatives of $\mathcal{X}$ (mod G),
   (b) the projection $\mathrm{E}(\mathcal{Y}) \to \mathrm{E}(G\backslash\mathcal{X})$ is a bijection, and
   (c) any edge of $\mathcal{Y}$ has at least one of its vertices in $\mathcal{S}$.

(2) An *edge pairing for a fundamental domain $\mathcal{Y}$ of $\mathcal{X}$ under G* is a map

$$\mathrm{PE} := \mathrm{PE}_{(\mathcal{S},\mathcal{Y})} := \{e \in \mathrm{E}(\mathcal{Y}) \setminus \mathrm{E}(\mathcal{S}) \mid o(e) \in \mathcal{S}\} \to G : e \mapsto g_e$$

   such that $g_e t(e) \in \mathrm{V}(\mathcal{S})$. We write PE for *paired edges*. To avoid cumbersome notation, we usually abbreviate $\mathrm{PE}_{\mathcal{Y},\mathcal{S}}$ by PE.

(3) An *enhanced fundamental domain for $\mathcal{X}$ under G* consists of a fundamental domain, an edge pairing and simplex labels $G_t := \mathrm{Stab}_G(t)$ for all simplices t of $\mathcal{Y}$.

An edge pairing encodes that under the G-action any $e = (v, v') \in \mathrm{PE}$ is identified (paired) with $ge = (g_e v, g_e v')$ when passing from $\mathcal{X}$ to $G\backslash\mathcal{X}$. Because $\mathcal{X}$ is a tree and the image of $\mathcal{S}$ in $G\backslash\mathcal{X}$ is a maximal subtree, each edge in $\mathrm{E}(\mathcal{Y}) \setminus \mathrm{E}(\mathcal{S})$ has exactly one of its vertices in $\mathrm{V}(\mathcal{S})$ and therefore PE contains exactly those edges of $\mathrm{E}(\mathcal{Y}) \setminus \mathrm{E}(\mathcal{S})$ pointing away from $\mathcal{S}$. An enhanced fundamental domain is a graph of groups in the sense of [Se1, I.4.4, Def. 8] realized inside $\mathcal{X}$. Given a fundamental domain with an edge pairing the tree $\mathcal{S}$ can be recovered from $\mathcal{Y}$ and PE.

Remark 6.3. If one barycentrically subdivides $\mathcal{T}$, an alternative way to think of an edge pairing is that it pairs the two half sides $[o(e), \frac{1}{2}o(e) + \frac{1}{2}t(e)]$ and $[g_e t(e), g_e(\frac{1}{2}o(e) + \frac{1}{2}t(e))]$.

It will be convenient to introduce the following notation:

Definition 6.4. For any group G acting on a set X we define a category $\mathcal{C}_G(X)$ whose objects are the elements of X and whose morphism sets are defined as

$$\mathrm{Hom}_G(x,y) := \{\gamma \in G \mid gx = y\} \subseteq G.$$

for $x, y \in X$. The composition of morphisms is given by multiplication in G.

In particular $\mathrm{End}_G(x) := \mathrm{Hom}_G(x,x) = \mathrm{Stab}_G(x)$.

For the remainder of this section, we assume that $\mathrm{Hom}_\Gamma(v,w)$ can be computed effectively for all $v, w \in \mathrm{V}(\mathcal{T})$. This will be studied in Section 7.

Algorithm 6.5. (Computation of the quotient graph)

Input: *A subgroup $\Gamma \subset \mathrm{GL}_2(K_\infty)$ for which there exists a routine for computing $\mathrm{Hom}_\Gamma(v,v')$ for all $v, v' \in \mathrm{V}(\mathcal{T})$ which are equidistant from $[L(0,0)]$.*

Output: *A directed multigraph $\mathcal{G}$ with a label attached to each simplex. The label values on edges are either $(e,1)$ (preset), or $(e,-1)$, or a pair (e,g) with $e \in \mathrm{E}(\mathcal{T})$, $g \in \Gamma$. The label values on vertices are either $(v,1)$ (preset) or (v,G) for $v \in \mathrm{V}(\mathcal{T})$ and $G \subset \Gamma$ a finite subgroup.*

Algorithm:

(1) Set $v_0 = [L(0,0)]$. If $\#\,\mathrm{End}_\Gamma(v_0) = q^2 - 1$, replace v_0 by $[L(1,0)]$. If after replacement we still have $\#\,\mathrm{End}_\Gamma(v_0) = q^2 - 1$, then terminate the algorithm with the output the connected graph on 2 vertices and one edge and with vertex labels $\mathrm{End}_\Gamma(v)$ for each of the two vertices v.

(2) Initialize a graph $\mathcal{G}$ with $\mathrm{V}(\mathcal{G}) = \{v_0\}$ and $\mathrm{E}(\mathcal{G}) = \emptyset$. Also, initialize lists $L := (e \in \mathrm{E}(\mathcal{T}) \mid o(e) = v_0)$, the edges adjacent to v_0, and $L' := \emptyset$. All vertices v of $\mathcal{T}$ are given by a matrix in vertex normal form $\mathrm{vnf}(v)$.

(3) While L is not empty:
  (a) For $i = 1$ to $\#L$ do:
    (i) Let $e = (v, v')$ be the ith element in L.
    (ii) Compute $\mathrm{End}_\Gamma(v')$.
    (iii) If $\#\,\mathrm{End}_\Gamma(v') = q^2 - 1$ then:
      (A) Add the vertex v' to $\mathrm{V}(\mathcal{G})$ and e and $e^\star$ to $\mathrm{E}(\mathcal{G})$.
      (B) Store $(v', \mathrm{End}_\Gamma(v'))$ as a vertex label for v'.
      (C) Remove e from L.
    (iv) If $\#\,\mathrm{End}_\Gamma(v') = q - 1$, then for all $j < i$ do the following:
      (A) Let $e' = (w, w')$ be the jth element in L.
      (B) Compute $\mathrm{Hom}_\Gamma(v', w')$.
      (C) If $\mathrm{Hom}_\Gamma(v', w') \neq \emptyset$, then do the following
        • Add an edge e' from v to w' to $\mathrm{E}(\mathcal{G})$, as well as its opposite.
        • Give e' the label (e, g_e) for some $g_e \in \mathrm{Hom}_\Gamma(v', w')$

and give $e'^{\star}$ the label $(e,-1)$.
- Remove (v,v') from L and set $j := i$.
- Remove $(w', \mathrm{vnf}(g_e v))$ from L'.
- If now $\deg_{\mathcal{G}}(w') = q+1$, then remove (w,w') from L.

(D) Continue with the next j.

(v) If at the end of the j-loop we have $j = i$, then:

(A) Add v' to $\mathrm{V}(\mathcal{G})$, add e and $e^{\star}$ to $\mathrm{E}(\mathcal{G})$.

(B) For all adjacent vertices $w \neq v$ of v' in $\mathcal{T}$ add (v',w) to L'.

(b) Set $L := L'$ and $L' := \emptyset$.

(4) If L is empty, return $\mathcal{G}$.

Remark 6.6. One could randomly choose a vertex $[L(n,g)]$ as v_0 and replace it by $[L(n+1,g)]$, if it is projectively unstable. In this case, one would need to change the input of Algorithm 6.5 accordingly.

Remark 6.7. The vertex label $(v,1)$ is used at all projectively stable vertices. For these, the stabilizer is the center of $\mathrm{GL}_2(K_\infty)$ intersected with Γ. There is no need to store this group each time. The same remark applies to all edge labels $(e,1)$.

A maximal subtree $\mathcal{S}$ of $\mathcal{G}$ consists of all vertices of $\mathcal{G}$ and those edges of $\mathcal{G}$ with edge label $(e,1)$. It is completely realized within $\mathcal{T}$.

The edges with label (e,g) are the edges which occur (ultimately) in PE. The edge label $(e,-1)$ indicates that the opposite edge has a label (e,g). It is clear that the vertex and edge label allow one to easily construct an enhanced fundamental domain $(\mathcal{S},\mathcal{Y})$ with an edge pairing and labels for the action of Γ on $\mathcal{T}$.

Theorem 6.8. *Suppose Γ from Algorithm 6.5 satisfies the following conditions:*

(1) *$d(v,gv)$ is even for all $g \in \Gamma, v \in \mathrm{V}(\mathcal{T})$,*
(2) *for simplices t of $\mathcal{T}$ either $\bar{\Gamma}_t$ is trivial, or t is a vertex and $\bar{\Gamma}_t \cong \mathbb{Z}/(q+1)$,*
(3) *$\Gamma\backslash\mathcal{T}$ is finite.*

Then Algorithm 6.5 terminates and computes an enhanced fundamental domain for $\mathcal{T}$ under Γ.

By the results in Section 5, hypotheses (a)–(c) are satisfied if Γ is the unit group of a maximal order of a quaternion algebra D as in Assumption 4.7.

Remark 6.9. Let us comment on the hypotheses made in Theorem 6.8 in order for Algorithm 6.5 to terminate: Following the example set by the number field case, it seems natural to consider the following situation: Let C be a smooth projective geometrically connected curve over $\mathbb{F}_q$, let S be

a finite set of closed points of C, set $A = \Gamma(C \setminus S, \mathcal{O}_C)$ and let $K = Q(A)$ be the fraction field of A. Let furthermore D denote a division algebra over K which is ramified at all but one point ∞ of S and let Λ be an A-order. As can be deduced in this situation from [Vi] by an argument similar to Proposition 4.11, the group Λ^* modulo its center acts discretely on the Bruhat-Tits tree for $\mathrm{PGL}_2(K_\infty)$. We expect but have not checked that hypotheses (1)–(3) of Theorem 6.8 are always met in this situation. What is missing in this general situation is an explicit algorithm to compute $\mathrm{Hom}_{\Lambda^*}(v, v')$. For this, see Remark 7.5.

Proof of Theorem 6.8. Let $\mathcal{G}$ be the output of Algorithm 6.5. We show that any two distinct simplices of $\mathcal{G}$ have labels $(t, ?)$ and $(t', ?)$ with $t' \notin \Gamma t$ and that for all simplices t of $\mathcal{T}$ there is a simplex of $\mathcal{G}$ whose label is $(t', ?)$ for some $t' \in \Gamma t$.

For the first assertion, let $v_1, v_2 \in \mathrm{V}(\mathcal{T})$ be distinct first entries in labels of vertices of $\mathcal{G}$ and suppose that $\gamma v_1 = v_2$ for some $\gamma \in \Gamma \setminus \Gamma_{v_1}$. We seek a contradiction. In a first reduction step we show that we may assume that v_1 is projectively stable: So suppose v_1 is projectively unstable. Then since

$$\mathrm{Stab}_\Gamma(v_2) = \gamma \,\mathrm{Stab}_\Gamma(v_1)\gamma^{-1}, \tag{6.1}$$

also v_2 has to be projectively unstable. Hence both v_1 and v_2 are terminal vertices in $\mathcal{G}$. Let v_1' and v_2' be their unique adjacent vertices in $\mathcal{G}$. Since v_1' is adjacent to v_1, it follows that $\gamma v_1'$ is adjacent to $\gamma v_1 = v_2$. By condition (b) the stabilizer $\mathrm{Stab}_\Gamma(v_2)$ acts transitively on the vertices adjacent to v_2. Hence there exists $\gamma' \in \mathrm{Stab}_\Gamma(v_2)$ with

$$\gamma'\gamma v_1' = v_2', \tag{6.2}$$

and so v_1' and v_2' are Γ-equivalent. If v_1' and v_2' were also projectively unstable and therefore terminal vertices in $\mathcal{G}$, then, since $\mathcal{G}$ is connected, $\mathcal{G}$ would have to be the graph consisting of the two vertices v_1, v_2 and one edge connecting them. This contradicts condition (a). Therefore v_1' and v_2' must be projectively stable and Γ-equivalent. To conclude the reduction, observe that we cannot have $v_1' = v_2'$, since in this case we must have $\gamma'\gamma \in \mathbb{F}_q^*$ from (6.2). But $\gamma'\gamma$ maps v_1 to v_2 and this would contradict $v_1 \neq v_2$.

Now suppose v_1 is projectively stable. Then by equation (6.1) so is v_2. Let v be the initial vertex of the algorithm and let $i_1 = d(v, v_1)$ and $i_2 = d(v, v_2)$. We prove the assertion by induction over i_1: If $i_1 = 1$ then also $i_2 = 1$ because of condition (a). Hence the vertices v_1 and v_2 both have the same distance 1 from v and since $\mathrm{Hom}_\Gamma(v_1, v_2) = q - 1$, Algorithm 6.5 with the first choice of L rules out that they both lie in $\mathcal{G}$. This is a contradiction. The same reasoning rules out $i_1 = i_2$ for any $i_1, i_2 \geq 1$.

Suppose $i_1 > 1$. By condition (a) and the previous line we may assume $i_1 = i_2 + 2m$ for some $m \in \mathbb{Z}_{\geq 1}$. Let v_1' be the vertex on the geodesic from v_1 to v so that $d(v, v_1') = i_1 - 1$. Then by the construction of $\mathcal{G}$ we

have $v_1' \in \mathcal{G}$. The vertex $\gamma v_1'$ is adjacent to $\gamma v_1 = v_2$. Now observe that $\gamma v_1'$ does not belong to $\mathcal{G}$ because otherwise we could apply the induction hypothesis to $v_1', \gamma v_1'$, using $d(v_1', v) = i_1 - 1$ and $d(\gamma v_1', v) \leq i_2 + 1$ to obtain a contradiction.

It follows that $v_2' := \gamma v_1' \notin \mathcal{G}$. Since by construction the geodesic from v to v_2 lies on $\mathcal{G}$, we have $d(v_2', v) = i_2 + 1$. Now by the algorithm that defines $\mathcal{G}$ the vertex v_2' must be equivalent to a vertex of distance $i_2 - 1$, i.e., there are $\gamma' \in \Gamma, v_2'' \in \mathcal{G}$ with $d(v_2'', v) = i_2 - 1$ such that $v_2'' = \gamma' v_2'$. But then we apply the induction hypothesis to v_1', v_2'' and again obtain a contradiction. This concludes the proof of the first assertion for vertices.

Suppose now that $e = (v_0, v_1), e' = (v_0', v_1')$ occur as first entries in $\mathrm{E}(\mathcal{G})$, lie in the same Γ-orbit, are distinct and occur in some edge labels of $\mathcal{G}$. Let γ be in Γ with $e' = \gamma e$. Note that not all the vertices v_i and v_i' must occur in vertex labels from $\mathcal{G}$ but each edge must at least have one vertex that does – see step (c)(i)4.C. Suppose after possibly changing the orientation of edges and the indices that v_0 has minimal distance from v. By construction of $\mathcal{G}$ the vertex v_0 occurs in a vertex label. If $v_0' = \gamma v_0$ occurs in a vertex label of $\mathcal{G}$, then by the case already treated, we must have $v_0 = v_0'$. Since $e \neq e'$ it follows that v_0 is projectively unstable. But then the algorithm does not yield an edge starting at v_0 and ending at a vertex v_1 with $d(v, v_1) > d(v, v_0)$. This is a contradiction.

It follows that $v_0' = \gamma v_0$ does not occur in a vertex label. Hence v_1' must occur in a vertex label. By essentially the argument just given, v_1 can also not occur in a vertex label. Hence (e, γ) must be an edge label and moreover $d(v, v_1') = d(v, v_0) + 1 = d(v, v_0') - 1$. But then in step (c)(i)4.C of Algorithm 6.5 the edge e' must have been removed from the list L' and so it cannot occur in a label of an edge of $\mathcal{G}$.

We finally come to the second assertion: By construction, $\mathcal{G}$ defines a connected graph. It is a subgraph of $\Gamma\backslash\mathcal{T}$, since we already showed that there are no Γ-equivalent simplices in $\mathcal{G}$. Moreover, at any vertex of this subgraph the degree within $\mathcal{G}$ and within $\Gamma\backslash\mathcal{T}$ is the same. Hence $\mathcal{G}$ defines a connected component of $\Gamma\backslash\mathcal{T}$. But $\mathcal{T}$ and hence $\Gamma\backslash\mathcal{T}$ are connected and thus $\mathcal{G} = \Gamma\backslash\mathcal{T}$. □

We further describe an algorithm to compute for any $v' \in \mathrm{V}(\mathcal{T})$ a Γ-equivalent vertex $v'' \in \mathcal{G}$. This can be done in time linear to the distance from v' to $\mathcal{G}$. For this algorithm we need the stabilizers of the terminal vertices of $\mathcal{G}$ and the elements $\gamma \in \mathrm{Hom}_\Gamma(v_i, v_j)$, which we both stored as vertex and edge labels during the computation of $\mathcal{G}$. We call this algorithm the reduction algorithm. We need to be able to do the following:

(1) Find the geodesic from v' to v. This was discussed in Remark 3.5.

(2) Determine the extremities of a given geodesic in $\mathcal{G}$. Since the vertices in $\mathcal{G}$ are all stored in the vertex normal form, this can be done in constant time.

Algorithm 6.10. (The reduction algorithm)
Input: $v' \in \mathrm{V}(\mathcal{T})$ *and* $\mathcal{G}$ *the output of Algorithm 6.5 with initial vertex* v.
Output: *A tuple* $(w, \gamma) \in \mathrm{V}(\mathcal{G}) \times \Gamma$ *with* $v' = \gamma w$.
Algorithm:

(1) Let $\mathcal{T}_0 : (v' = v_m, v_{m-1}, \ldots, v)$ be the geodesic from v' to v. Let v_i be the vertex of $\mathcal{T}_0 \cap \mathcal{G}$ closest to v'. Let $r = m - i$, this is the distance from v' to $\mathcal{G}$.
(2) If $r = 0$, we have $v' \in \mathcal{G}$. Then return $(v', 1)$.
(3) If $r > 0$, we distinguish two cases:
   (a) If v_i is projectively unstable, by a for-loop through the elements γ in $\mathrm{Stab}_\Gamma(v_i)$, find an element $\gamma \in \Gamma$ such that γv_{i+1} is a vertex of $\mathcal{G}$. Replace v' by $\gamma v'$ and apply the algorithm recursively to get some pair $(w, \tilde{\gamma})$ in $\mathrm{V}(\mathcal{G}) \times \Gamma$. Return $(w, \tilde{\gamma}\gamma)$.
   (b) If v_i is projectively stable, run a for-loop through the vertices $\tilde{v}$ in $\mathcal{G}$ adjacent to v_i to find the unique $\tilde{v}$ such that either: (i), the edge label of the edge from $\tilde{v}$ to v_i is of the form (e, γ) for some $\gamma \in \Gamma$ with $\gamma t(e) = v_i$ and $\gamma o(e) = v_{i+1}$, or (ii), the edge label from v_i to $\tilde{v}$ is of the form (e, γ) for some $\gamma \in \Gamma$ with $o(e) = v_i$ and $t(e) = v_{i+1}$. In case (i), replace v' by $\gamma^{-1}v'$ and apply the algorithm recursively to get some pair $(w, \tilde{\gamma})$ for $\gamma^{-1}v'$. Return $(w, \tilde{\gamma}\gamma^{-1})$. In case (ii), replace v' by $\gamma v'$ and apply the algorithm recursively to get some pair $(w, \tilde{\gamma})$ for $\gamma v'$. Return $(w, \tilde{\gamma}\gamma)$.

Proposition 6.11. *Let* v' *in* $\mathcal{T}$ *and let* $\mathcal{G}$ *be the output of Algorithm 6.5 under the hypothesis of Theorem 6.8 with initial vertex* v. *Then Algorithm 6.10 computes a* Γ*-equivalent vertex* w *of* v' *and an element* $\gamma \in \Gamma$ *with* $\gamma v' = w$. *It requires* $\mathcal{O}(n^3 \deg(r)^2)$ *additions and multiplications in* $\mathbb{F}_q$ *where* n *is the distance of* v' *to* $\mathcal{G}$.

Proof. In both cases of the algorithm we find an edge label that moves v' closer to $\mathcal{G}$. Since each step of the algorithm decreases the distance $d(v', \mathcal{G})$, the algorithm terminates after at most n steps. From Corollary 9.5 and Proposition 4.14 it follows that at step j one multiplies a matrix of height $(j-1)\frac{5}{2}\deg(r)$ with one of height $\frac{5}{2}\deg(r)$. Further one has to compute the vertex normal form of a matrix of height at most $(j+1)\frac{5}{2}\deg(r)$. This takes at most $(8j + 8j^2)\frac{5}{2}^2 \deg(r)^2$ operations in $\mathbb{F}_q$. Summing over j, the asserted bound follows. □

Example 6.12. In Figure 6.1 we give an example of the Algorithm 6.5, where $q = 5$ and $r = T(T+1)(T+2)(T+3)$. We start with $\begin{pmatrix} 1/T & 0 \\ 0 & 1 \end{pmatrix}$ as the initial vertex v. The adjacent vertices correspond to the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, which is a terminal vertex, and the five matrices $\begin{pmatrix} 1/T^2 & \alpha 1/T \\ 0 & 1 \end{pmatrix}$ with $\alpha \in \mathbb{F}_5$. Using the algorithm described in Section 7 we compute that $\begin{pmatrix} 1/T^2 & 0 \\ 0 & 1 \end{pmatrix}$ is the only projectively unstable vertex and

$$\#\operatorname{Hom}_\Gamma(\begin{pmatrix} 1/T^2 & 1/T \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1/T^2 & 41/T \\ 0 & 1 \end{pmatrix}) = 4,$$

$$\#\operatorname{Hom}_\Gamma(\begin{pmatrix} 1/T^2 & 2\pi \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1/T^2 & 3\pi \\ 0 & 1 \end{pmatrix}) = 4.$$

This finishes Step 1 of the algorithm, as depicted in Figure 6.1. In Step 2 we then continue with the eight indicated vertices of level 3. In this case, the algorithm terminates after 3 steps.

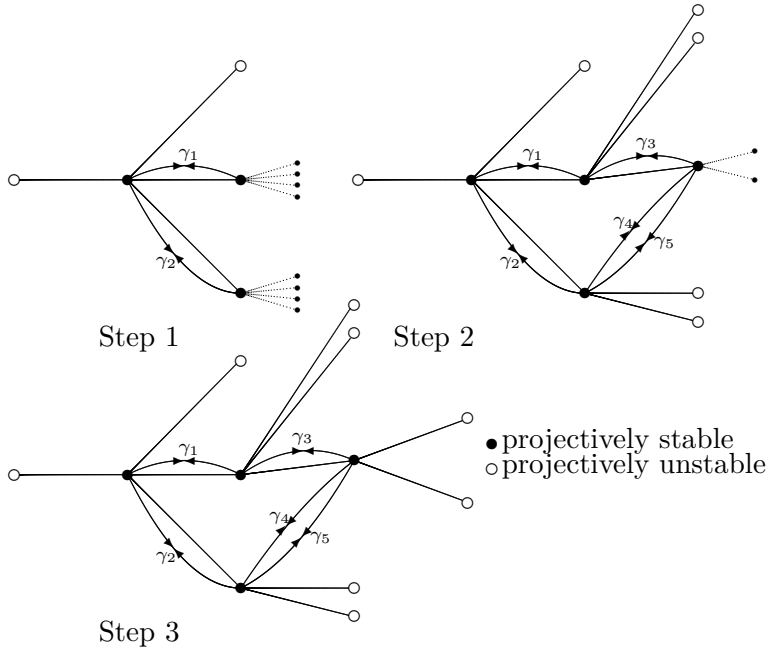

FIGURE 6.1. Example: $q = 5$, $r = T(T+1)(T+2)(T+3)$

Example 6.13. Consider $K = \mathbb{F}_5(T)$ and the two discriminants $r_1 = (T^2+T+1)\cdot T\cdot(T+1)\cdot(T+2)$ and $r_2 = (T^2+2)\cdot T\cdot(T+1)\cdot(T+2)$.

Let Γ_i be the group of units of a maximal order of a quaternion algebra of discriminant r_i for $i \in \{1,2\}$. Then $\Gamma_1\backslash\mathcal{T}$ has 14 cycles of length 2, while $\Gamma_2\backslash\mathcal{T}$ has 10 cycles of length 2. Hence these two graphs are not isomorphic. This answers a question of Papikian who asked for an example in which the lists of degrees of the factors of r and r' are the same but where the graphs are non-isomorphic. This is similar to [GN, Rem 2.22] where congruence subgroups $\Gamma_0(\mathfrak{n})$ and $\Gamma_0(\mathfrak{n}')$ of $\mathrm{GL}_2(A)$ are considered.

7. Computing $\mathrm{Hom}_\Gamma(v,w)$

Let $r, \alpha, \Lambda \subset D = \left(\frac{\alpha,r}{K}\right), \iota$ be as at the end of Section 4; recall also that $\pi = 1/T$ is a uniformizer of K_∞.

Lemma 7.1. *To compute $\sqrt{\alpha}$ in $K_\infty = \mathbb{F}_q((\pi))$ to n digits of accuracy one requires $\mathcal{O}(n^3)$ additions and multiplications in $\mathbb{F}_q$.*

Proof. Let $m = \deg(\alpha)$. It suffices to compute the square root u of the 1-unit $\pi^m\alpha$ to n digits accuracy. This can be done by the Newton iteration in n steps starting with the approximation $u_0 = 1$. The k-th approximation is $u_k = u_{k-1} - \frac{u_{k-1}^2 - \pi^m\alpha}{u_{k-1}}$. From the right hand expression one only needs to compute $u_{k-1}^2 - \pi^m\alpha$ which requires n^2 operations in $\mathbb{F}_q$. The k-th digit past the decimal point divided by 2 has then to be subtracted from u_{k-1}. □

To state the following result, we define a (logarithmic) height $\|\ \|$ on elements of Λ. Its definition will be in terms of our standard A-basis of Λ, and it will depend on this choice. For $(\lambda_1,\lambda_2,\lambda_3,\lambda_4) \in A^4$ we define

$$\|\lambda_1\cdot 1 + \lambda_2\cdot i + \lambda_3\cdot j + \lambda_4\cdot\frac{\varepsilon i + ij}{\alpha}\| := \max_{i\in\{1,2,3,4\}} \deg(\lambda_i). \tag{7.1}$$

We also define, as an abbreviation, v_∞ applied to a matrix or a vector of elements in K_∞ to be the minimum of all the v_∞-valuations of all entries.

Theorem 7.2. *Suppose $v, v' \in \mathrm{V}(\mathcal{T})$ have distance n from $v_0 = [L(0,0)]$.*

1. *There is an algorithm that computes $\mathrm{Hom}_\Gamma(v,v')$ in time $\mathcal{O}(n^4)$ field operations over $\mathbb{F}_q$.*
2. *All $\gamma \in \mathrm{Hom}_\Gamma(v,v')$ satisfy $\|\gamma\| \le n + \deg(\alpha)/2$.*

Proof. If $v = [L(l,g)]$ has distance n from v_0, then either

$$l = n \quad \text{and} \quad \deg_l(g) \text{ lies in } \{0,\dots,n\} \text{ or}$$
$$l \in \{-n, -n+2, -n+4, \dots, n-2\} \quad \text{and} \quad \deg_l(g) = \frac{n+l}{2},$$

see Figure 3.1 and Remark 3.5. Moreover the path from $[L(0,0)]$ to $[L(l,g)]$ is via $L(\frac{l-n}{2}, 0)$ if $l < n$ and via $L(n - \deg_l(g), 0)$ if $l = n$. Set $n_1 := \deg_l(g)$ and $n_2 := n - n_1$ if $l = n$ and $n_2 = n_1 - n$ if $l < n$. In Figure 3.1, the integers n_1 and $n_2 \in \mathbb{Z}$ are the coordinates of v from the baseline toward it and along

the baseline, respectively. Moreover $l = n_1+n_2$ and $g \in \pi^{l-n_1}\mathcal{O}_\infty = \pi^{n_2}\mathcal{O}_\infty$. Similarly we define n_1' and n_2' for $v' = [L(l', g')]$ which is also of distance n from $v_0 = [L(0,0)]$.

Let now $\gamma = \begin{pmatrix} \pi^l & g \\ 0 & 1 \end{pmatrix}$ and $\gamma' = \begin{pmatrix} \pi^{l'} & g' \\ 0 & 1 \end{pmatrix}$ be the matrices in vertex normal form representing v and v' respectively. By definition of Hom_Γ we have

$$\mathrm{Hom}_\Gamma(v, v') = \gamma' \mathrm{GL}_2(\mathcal{O}_\infty) K_\infty^* \gamma^{-1} \cap \Gamma.$$

Because $v_\infty(\det(\gamma)) = l, v_\infty(\det((\gamma')^{-1}) = l'$, $v_\infty(\det(\sigma)) = 0$ for all $\sigma \in \mathrm{GL}_2(\mathcal{O}_\infty)$ and $v(\det \Gamma) = \{0\}$, we see that

$$\mathrm{Hom}_\Gamma(v, v') = \pi^{(l-l')/2} \gamma' \mathrm{GL}_2(\mathcal{O}_\infty) \gamma^{-1} \cap \Gamma,$$

where we simply write $\pi^{(l-l')/2}$ for the scalar matrix $\pi^{(l-l')/2} \cdot 1_2$. By taking determinants on both sides and using the fact that $\mathcal{O}_\infty \cap A = \mathbb{F}_q$, we finally obtain

$$\mathrm{Hom}_\Gamma(v, v') \overset{\bullet}{\cup} \{0\} = \pi^{(l-l')/2} \gamma' M_2(\mathcal{O}_\infty) \gamma^{-1} \cap \Lambda. \tag{7.2}$$

Equation (7.2) can be interpreted in the following way: The intersection in (7.2) is up to change by conjugation the same as $M_2(\mathcal{O}_\infty) \cap \pi^{(l'-l)/2} \gamma'^{-1} \Lambda \gamma$. Here $M_2(\mathcal{O}_\infty)$ is the unit ball in $M_2(K_\infty)$, a K_∞-vector space of dimension 4 and $\pi^{(l'-l)/2} \gamma'^{-1} \Lambda \gamma$ is a discrete A-lattice (of rank 4) in this vector space. I.e., we need to compute the shortest non-zero vectors of the lattice $\pi^{(l'-l)/2} \gamma'^{-1} \Lambda \gamma$ with respect to the norm given by $M_2(\mathcal{O}_\infty)$. If these vectors have norm at most one, they form $\mathrm{Hom}_\Gamma(v, v')$. If their norm is larger than one, then $\mathrm{Hom}_\Gamma(v, v')$ is empty. In particular, the problem can in principle be solved by the function field version of the LLL algorithm.

However, the implemented versions of the LLL algorithm [He, Pau] need an a priori knowledge of the precision by which α has to be computed as an element in $\mathbb{F}_q((\pi))$. This in turn makes it necessary to find a bound on the height of the elements in $\mathrm{Hom}_\Gamma(v, v')$, if described as a linear combination in terms of our standard A-basis for Λ. Moreover, [He, Pau] do not give a complexity analysis for their algorithms. To derive these quantities, i.e. precision, height and complexity, we proceed as follows. Set

$$C = \begin{pmatrix} 1 & \sqrt{\alpha} & 0 & \frac{\epsilon}{\sqrt{\alpha}} \\ 0 & 0 & 1 & \frac{1}{\sqrt{\alpha}} \\ 0 & 0 & r & \frac{-r}{\sqrt{\alpha}} \\ 1 & -\sqrt{\alpha} & 0 & \frac{-\epsilon}{\sqrt{\alpha}} \end{pmatrix} \text{ and } B = \begin{pmatrix} \pi^{\frac{l'-l}{2}} & 0 & g'\pi^{\frac{-l'-l}{2}} & 0 \\ -g\pi^{\frac{l'-l}{2}} & \pi^{\frac{l'+l}{2}} & -gg'\pi^{\frac{-l'-l}{2}} & g'\pi^{\frac{l-l'}{2}} \\ 0 & 0 & \pi^{\frac{-l'-l}{2}} & 0 \\ 0 & 0 & -g\pi^{\frac{-l'-l}{2}} & \pi^{\frac{l-l'}{2}} \end{pmatrix}.$$

Observe that $v_\infty(g\pi^{-\frac{l}{2}}) \geq n_2 - \frac{n_1+n_2}{2} = \frac{n_2-n_1}{2} \geq -\frac{n}{2}$ and that $-|l| \geq -n$. This implies that $v_\infty(B) \geq -n$. Similarly, using $\deg(\varepsilon) \leq \deg(\alpha)$ and

computing C^{-1} explicitly, one finds $v_\infty(C^{-1}) \geq -m$ where we abbreviate $m := \frac{\deg(\alpha)}{2} \in \mathbb{Z}_{\geq 1}$.

We now flatten 2×2-matrices in $M_2(K_\infty)$ to column vectors of length 4. Taking the explicit form of the A-basis of Λ from Lemma 4.17 into account, as well as the explicit forms of γ and γ', the solutions to (7.2) are the solution of the linear system of equations

$$C\underline{\lambda} = B\underline{x}, \tag{7.3}$$

where $\underline{\lambda}$ denotes a (column) vector in A^4 and $\underline{x}$ a (column) vector in $\mathcal{O}_\infty^4$. The equivalent form $\underline{\lambda} = C^{-1}B\underline{x}$ and the above estimates on the valuations of C^{-1} and B now immediately imply $v_\infty(\underline{\lambda}) \geq -(n+m)$. In other words, the components of $\underline{\lambda}$ are polynomials and $\|\underline{\lambda}\| \leq n+m$. This proves (b).

Next, consider (7.3) in the form $B^{-1}C\underline{\lambda} = \underline{x}$. Again by explicit computation, we have $v_\infty(B^{-1}) \geq -n$ and $v_\infty(C) \geq -\max\{\deg(r), m\} =: -d$. Writing $B^{-1}C = \sum_{k=-d}^{\infty} X_k \pi^k$ as a power series with $X_k \in M_4(\mathbb{F}_q)$ and using the bound from (b), equation (7.3) is equivalent to

$$\big(\textstyle\sum_{k=-(n+m)}^{n+d} X_k \pi^{-k}\big)\underline{\lambda} \equiv 0 \pmod{\mathcal{O}_\infty^4}.$$

We also expand $\underline{\lambda} = \sum_{k=0}^{n+m} \underline{\lambda}_k \pi^{-k}$ as a polynomial in π^{-1} with $\underline{\lambda}_k \in {\mathbb{F}_q}^4$ and let X_k and $\underline{\lambda}_k$ be zero outside the range of indices k indicated above. Then (7.3) becomes equivalent to the system of linear equations

$$\big(\textstyle\sum_{k=0}^{n+m} X_{h-k}\underline{\lambda}_k\big) = 0, \quad h = 0, \ldots, 2n+d+m$$

in the indeterminates $\underline{\lambda}_k$ and with coefficients in $\mathbb{F}_q$. (Each equation has 4 linear components.) On the one hand, this shows that we need to compute α to accuracy $n' = 2n+d+m+1$. On the other hand, we see that, using Gauss elimination, one can solve for the unknowns in $\mathcal{O}({n'}^2)$ steps where each step consists of $(4n')^2$ additions and $(4n')^2$ multiplications in the field $\mathbb{F}_q$. Regarding $\deg(r)$ as a structural constant and applying Proposition 4.14, the complexity is thus $\mathcal{O}(n^4)$. □

Remark 7.3. We have chosen v_0 as a reference vertex in Theorem 7.2 for simplicity. Since $\mathrm{GL}_2(K_\infty)$ acts transitively on $\mathcal{T}$, one could work with any reference vertex. Also, if one chooses v_0 as the mid point of the geodesic from v to v', one sees that the complexity of an algorithm to compute $\mathrm{Hom}_\Gamma(v, v')$ is $\mathcal{O}(d^4)$ where $d = d(v, v')$. Note that only vertices that are an even distance apart can have non-trivial $\mathrm{Hom}_\Gamma(v, v')$, because $d(v, \gamma v)$ is even for all $\gamma \in \Gamma$ and $v \in \mathcal{T}$.

Remark 7.4. Our implementation of algorithm of Theorem 7.2 uses the Gauss algorithm and not LLL. The linear system that needs to be solved has $4n'$ equations in $4n + 2\deg(\alpha)$ variables with n' as in the above proof. In practice, $\deg(\alpha) \leq \deg(r)$, compare Proposition 4.14. As we shall see in Proposition 9.4, see also Remark 9.6, we have $n \leq 2\deg(r) - 2$ and typically

$\leq 2\deg(r)-4$. Therefore we have about $4n' \leq 22\deg(r)$ equations in about $10\deg(r)$ variables. Since the number of vertices of the quotient graph is essentially $q^{\deg(r)-3}$ (and $q \geq 3$), already $\deg(r) = 10$ is a large value to compute the entire graph. Over finite fields, systems of the size just described can be solved rather rapidly.

Remark 7.5. To adapt the algorithm of Theorem 7.2 to the generality proposed in Remark 6.9 at this point requires substantial new code for function fields. Using the notation from there, the rings A tend not to be UFD's and thus have a more sophisticated arithmetic. Moreover we do not expect that one should be able to give explicit simple formulas that describe the quaternion algebra D and even less so a maximal order Λ in it. One could work with non-maximal orders $\widetilde{\Lambda}$ but the quotient graph $\widetilde{\Lambda}^*\backslash\mathcal{T}$ has typically much larger size than $\Lambda^*\backslash\mathcal{T}$. If one has a reasonably simple description of Λ then an algorithm as in Theorem 7.2 should be doable (certainly in the case where S consists of one place only). Also, as far as we are aware of, an LLL algorithm in this generality is not implemented. Because of all these still open problems, it seems reasonable to present the algorithm here for $\mathbb{F}_q[T]$ only.

8. Presentations of Γ and the word problem

From a fundamental domain for the action of Γ on $\mathcal{T}$ together with a side pairing one obtains a presentation of Γ as an abstract group. This has been explained in [Se1, Chapter I.4] interpreting Γ as the amalgam of the stabilizers of the vertices of $\Gamma\backslash\mathcal{T}$ along the stabilizers of the edges connecting them. Compare also [Pa1, Thm. 5.7].

Lemma 8.1 ([Se1, I.4.1, Lem. 4])**.** *Let G be a group acting on a connected graph $\mathcal{X}$ and $\mathcal{Y}$ a fundamental domain for the action of G on $\mathcal{X}$ with an edge pairing* PE*. Then G is generated by*

$$\{g_e \in e \in \mathrm{PE}\} \cup \{\mathrm{Stab}_G(v) \mid v \in \mathrm{V}(\mathcal{S})\}.$$

The relations among the generators of the previous lemma are given by [Se1, § I.5, Thm. 13] and based on the construction of the fundamental group $\pi(\Gamma, \mathcal{Y}, \mathcal{S})$ in [Se1, p. 42]. For the group Γ considered here, all non-terminal vertices v of $\mathcal{S}$ have stabilizer $\mathbb{F}_q^*$ which lies in the center of Γ. The results just quoted therefore considerably simplify and yield:

Proposition 8.2. *Let $(\mathcal{Y}, \mathcal{S}, (g_e)_{e\in\mathrm{PE}})$ be a fundamental domain with an edge pairing for $(\Gamma, \mathcal{T})$ as provided by Algorithm 6.5. For each terminal vertex $v \in \mathrm{V}(\mathcal{S})$, let g_v be a generator of* $\mathrm{Stab}_\Gamma(v)$*. Then Γ is isomorphic to the group generated by*

$$\{g_0\} \cup \{g_v \mid v \text{ terminal in } \mathrm{V}(\mathcal{S})\} \cup \{g_e \text{ the edge-label} \mid e \in \mathrm{PE}\}$$

subject to the relations

$$g_0^{q-1} = 1,\ g_v^{q+1} = g_0 \text{ for all terminal } v,\ [g_e, g_0] = 1 \text{ for all } e \in \mathrm{PE}\,.$$

In particular g_0 lies in the center of Γ, as it should.

Example 8.3. In Example 6.12 the group Γ is generated by

$$\{g_0, g_{v_1}, \dots, g_{v_8}, g_1, \dots, g_5\}$$

with relations

$$g_0^4 = 1, g_{v_i}^6 = g_0, [g_0, g_i] = 1.$$

The word problem with respect to this set of generators was already solved by the reduction Algorithm 6.10, compare [Vo, Remark 4.6].

9. Complexity analysis and degree bounds

In this section we will analyze the complexity of Algorithm 6.5 and obtain some bounds on the size of generators of Γ. We start by bounding the diameter of the graph $\Gamma\backslash\mathcal{T}$. The idea of using the Ramanujan property to obtain complexity bounds was inspired by [KV, Conj. 6.6]. A standard reference is [Lu].

Definition 9.1. A k-regular connected graph $\mathcal{G}$ is called a *Ramanujan graph* if for every eigenvalue λ of the adjacency matrix of $\mathcal{G}$ either $\lambda = \pm k$ or $|\lambda| \leq 2\sqrt{k-1}$.

Proposition 9.2 ([Lu, Prop 7.3.11])**.** *Let $\mathcal{G}$ be a k-regular Ramanujan graph on $n \geq 3$ vertices.*[1] *Then*

$$\mathrm{diam}(\mathcal{G}) \leq \log_{k-1}(4n^2).$$

Let

$$\mathrm{one}(R) := \begin{cases} 1 & \text{if some place in } R \text{ has degree one,} \\ q(q-1) & \text{otherwise.} \end{cases}$$

Lemma 9.3. *There is a covering of $\mathcal{G} := \Gamma\backslash\mathcal{T}$ by a $q+1$-regular Ramanujan graph $\tilde{\mathcal{G}}$ with*

$$\#\,\mathrm{V}(\tilde{\mathcal{G}}) = \frac{2\,\mathrm{one}(R)}{(q-1)^2} \prod_{\mathfrak{p} \in R} (q_{\mathfrak{p}} - 1).$$

Proof. Recall the definitions and formulas for V_1 and V_{q+1} from Theorem 5.6. If $\mathrm{one}(R) = 1$, we can choose a degree 1 place $\mathfrak{p}_0 \in R$. If not we choose an arbitray degree 1 prime $\mathfrak{p}_0$. Let $\Gamma(\mathfrak{p}_0)$ be the full level $\mathfrak{p}_0$ congruence subgroup in Γ. By [LSV, Thm. 1.2] we know that $\tilde{\mathcal{G}} := (\Gamma \cap \Gamma(\mathfrak{p}_0))\backslash\mathcal{T}$ is a Ramanujan graph. Observe that $(\Gamma \cap \Gamma(\mathfrak{p}_0))\backslash\Gamma \cong \mathbb{F}_{q^2}^*$ if $\mathfrak{p}_0 \in R$, which

[1] The proof in [Lu] requires at least one eigenvalue λ of the adjacency matrix with $|\lambda| \leq 2\sqrt{k-1}$ and hence $n \geq 3$. Also, the assertion is obviously wrong for $n = 2$ and k large.

has cardinality q^2-1, and $(\Gamma \cap \Gamma(\mathfrak{p}_0))\backslash\Gamma \cong \mathrm{GL}_2(\mathbb{F}_q)$ otherwise, which has cardinality $\mathrm{one}(R)(q^2-1)$. By analyzing the growth of the stabilizers from $\Gamma \cap \Gamma(\mathfrak{p}_0)$ to Γ, we observe that

$$\begin{aligned}\frac{1}{\mathrm{one}(R)} \# \mathrm{V}(\tilde{\mathcal{G}}) &= V_1 + (q+1)V_{q+1} \\ &= \Big(V_1 + \frac{q+1}{q-1}V_1 + \frac{2(q+1)}{q-1}(g(R)-1)\Big) \\ &= \frac{2}{(q-1)^2}\prod_{\mathfrak{p}\in R}(q_{\mathfrak{p}}-1).\end{aligned}$$

□

Proposition 9.4. *Suppose* $\mathrm{V}(\Gamma\backslash\mathcal{T}) \geq 3$. *Then*

$$\mathrm{diam}(\Gamma\backslash\mathcal{T}) \leq 2\deg(r) + 2(2\log_q(2) + 1 - \log_q(q-1)).$$

Proof. Let $\mathcal{G} = \Gamma\backslash\mathcal{T}$ and $\mathcal{G}'$ be the covering from Lemma 9.3. Then

$$\begin{aligned}\mathrm{diam}(\mathcal{G}) \;\leq\; \mathrm{diam}(\mathcal{G}') &\overset{9.2}{\leq} 2\log_q(\#\,\mathrm{V}(\mathcal{G}')) + \log_q(4) \\ &\overset{9.3}{\leq} 2\log_q\Big(\frac{2q}{q-1}\prod_{\mathfrak{p}\in R}(q_{\mathfrak{p}}-1)\Big) + \log_q(4) \\ &\leq 4\log_q(2) + 2\log_q(\frac{q}{q-1}) + 2\log_q\big(\prod_{\mathfrak{p}\in R} q_{\mathfrak{p}}\big) \\ &= 2(2\log_q(2) + 1 - \log_q(q-1)) + 2\deg(r).\end{aligned}$$

□

Corollary 9.5. *With* $\|\,\|$ *as in (7.1), the group* Γ *is generated by the set*

$$\{\gamma \in \Gamma \mid \|\gamma\| \leq \deg(\alpha)/2 + 2\deg(r) + 2(2\log_q(2) + 1 - \log_q(q-1))\}.$$

Proof. By Proposition 8.2, the group Γ is generated by the vertex and edge labels of the quotient graph from Algorithm 6.5. By Proposition 7.2 these labels g_t have norm $\|g_t\| \leq \deg(\alpha)/2 + n$, where n is the distance in $\Gamma\backslash\mathcal{T}$ between the initial vertex and the labeled vertex. In particular, $n \leq \mathrm{diam}(\Gamma\backslash\mathcal{T})$. □

Remark 9.6. If $\mathrm{one}(R) = 1$, we can obviously subtract $2 + 2\log_q(q-1)$ from the diameter in Proposition 9.4 and subsequently from the bounds in Corollary 9.5. In the other case we expect this to be possible as well. This should follow by replacing $\Gamma(\mathfrak{p}_0)$ by

$$\tilde{\Gamma}_1(\mathfrak{p}_0) := \{\gamma \in \Gamma \mid \gamma \equiv \begin{pmatrix} 1 & \star \\ 0 & \star \end{pmatrix} \pmod{\mathfrak{p}_0} \text{ in } \mathrm{GL}_2(\mathbb{F}_q)\}.$$

Unfortunately we could not find this analog of [LSV, Thm. 1.2] for a congruence subgroup other than $\Gamma(\mathfrak{p})$ in the literature although it seems likely to hold.

If this was indeed true, we would obtain the improved bound

$$\operatorname{diam}(\Gamma\backslash\mathcal{T}) \leq 2\deg(r) + 4\log_q(2) - 4\log_q(q-1).$$

For $q > 19$ it gives $\operatorname{diam}(\Gamma\backslash\mathcal{T}) \leq 2\deg(r) - 4$. The nice feature of this last bound is that it was assumed in many concrete examples that we have computed.

Proposition 9.7. *Algorithm 6.5 computes the quotient graph $\Gamma\backslash\mathcal{T}$ in time*

$$\mathcal{O}((\#\,\mathrm{V}(\Gamma\backslash\mathcal{T}))^2 \operatorname{diam}(\Gamma\backslash\mathcal{T})^5) \overset{5.6}{=} \mathcal{O}(q^{2\deg(r)-6} \cdot \deg(r)^5)$$

in terms of operations over $\mathbb{F}_q$.

Proof. According to Prop 7.2, comparing two vertices in the algorithm can be done in time $\mathcal{O}(n^4)$, where n is always less or equal then $\operatorname{diam}(\Gamma\backslash\mathcal{T})$. The list of vertices in each step of the algorithm is always shorter than the cardinality of $\mathrm{V}(\Gamma\backslash\mathcal{T})$, so in each step the number of comparisons is bounded by $(\#\,\mathrm{V}(\Gamma\backslash\mathcal{T}))^2$. The number of steps is bounded by $\operatorname{diam}(\Gamma\backslash\mathcal{T})$ and the result follows. □

References

[BCP] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language.* J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[Bu] R. Butenuth, *Quaternionic Drinfeld modular forms.* PhD thesis, in preparation.

[Cr] J. Cremona, *The elliptic curve database for conductors to 130000.* Algorithmic number theory (Berlin, 2006), Lecture Notes Comp. Sci. **4076**, 11–29. Springer, Berlin, 2006.

[De] L. Dembélé, *Quaternionic Manin symbols, Brandt matrices and Hilbert modular forms.* Math. Comp. **76** (2007), no. 258, 1039–1057.

[GN] E.-U. Gekeler, U. Nonnengardt, *Fundamental domains of some arithmetic groups over function fields.* Int. J. Math. **6** (1995), 689–708.

[GV] M. Greenberg, J. Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms.* Accepted in Math. Comp.

[GY] P. Gunnells, D. Yasaki, *Hecke operators and Hilbert modular forms.* Algorithmic number theory (Berlin, 2008), Lecture Notes Comp. Sci. **5011**, 387–401. Springer, Berlin, 2008.

[He] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics* J. Symbolic Computation **33** (2002), no. 4, 425–445.

[JS] J. C. Jantzen, J. Schwermer, *Algebra.* Springer-Lehrbuch, 2006.

[KV] M. Kirschmer, J. Voight, *Algorithmic enumeration of ideal classes for quaternion orders.* SIAM J. Comput. **39** (2010), no. 5, 1714–1747.

[Lu] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures.* Birkhäuser, 1993.

[LSV] A. Lubotzky, B. Samuels, U. Vishne, *Ramanujan complexes of type $\tilde{A}_d^*$.* Israel J. Math. **149** (2005), 267–299.

[MS] V. K. Murty, J. Scherk, *Effective versions of the Chebotarev density theorem for function fields.* C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), no. 6, 523–528.

[Pa1] M. Papikian, *Local diophantine properties of modular curves of $\mathcal{D}$-elliptic sheaves.* Accepted in J. reine angew. Math.

[Pa2] M. Papikian, *On generators of arithmetic groups over function fields*. Accepted in International Journal of Number Theory.
[Pau] S. Paulus, *Lattice basis reduction in function fields*. Proceedings of the Third Symposium on Algorithmic Number Theory, ANTS-III (1998), LNCS **1423**, 567–575.
[Ro] M. Rosen, *Number theory in function fields*. GTM **210**. Springer, Berlin-New York, 2002.
[Se1] J.-P. Serre, *Trees*. Springer, Berlin-New York, 1980.
[Se2] J.-P. Serre, *A course in arithmetic*. GTM **7**. Springer, Berlin-New York, 1973.
[Te1] J.T. Teitelbaum, *The Poisson Kernel For Drinfeld Modular Curves*. J.A.M.S. **4** (1991), 491–511.
[Te2] J.T. Teitelbaum, *Modular symbols for A*. Duke Math. J. **68** (1992), 271–295.
[Sti] H. Stichtenoth, *Algebraic Function Fields and Codes*. GTM **254**, Springer, Berlin-New York, (2009).
[Ste] W. Stein, *Modular forms database*, (2004). `http://modular.math.washington.edu/Tables`.
[Vi] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions*. Lecture Notes in Math. **800**. Springer, Berlin, 1980.
[Vo] J. Voight, *Computing fundamental domains for Fuchsian groups*. J. Théor. Nombres Bordeaux **21** (2009), 469–491.

Gebhard Böckle

Ralf Butenuth

Interdisziplinäres Zentrum für wissenschaftliches Rechnen
Im Neuenheimer Feld 368
69120 Heidelberg, Germany
E-mail: `boeckle@uni-hd.de`
E-mail: `ralf.butenuth@iwr.uni-heidelberg.de`
URL: `http://www.iwr.uni-heidelberg.de/groups/arith-geom`