ARTICLE IN PRESS

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Computational Section

# A reduction algorithm for Hilbert modular groups ☆

Fredrik Strömberg

*School of Mathematical Sciences, The University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom*

ARTICLE INFO

*Article history:*
Received 24 November 2021
Received in revised form 14 February 2022
Accepted 21 February 2022
Available online xxxx
Communicated by S.J. Miller

*MSC:*
11F06
11F41
11Y35

*Keywords:*
Hilbert modular groups
Fundamental domains
Reduction theory

ABSTRACT

The aim of this paper is to present an explicit reduction algorithm for Hilbert modular groups over arbitrary totally real number fields. An implementation of the algorithm is available to download from [20]. The exposition is self-contained and sufficient details are given for the reader to understand how it works and implement their own version if desired.

© 2022 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

Given a group $G$, acting on a topological space $X$, it is often useful to have a set of representatives of the orbit, $G\backslash X$, which are "reduced" with respect to some suitable definition. In number theory the most prominent example is the reduction theory of the modular group $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$. This gives rise to a large number of interesting applications

☆ This work was supported by the Engineering and Physical Sciences Research Council [EP/N007360/1] and [EP/V026321/1].

*E-mail address:* fredrik.stromberg@nottingham.ac.uk.

https://doi.org/10.1016/j.jnt.2022.02.011

0022-314X/© 2022 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

including the classical theory of Gauss for binary quadratic forms and continued fractions, as well as more recent developments in modular and automorphic forms.

In the case of the modular group the topological space can be viewed as the complex upper-half plane $\mathbb{H} = \{z = x + iy \in \mathbb{C} \mid y > 0\}$ and the action is given by Möbius transformations. The most commonly used set of representatives of $\Gamma\backslash\mathbb{H}$ is given by the following set

$$\mathcal{F} = \{z = x + iy \in \mathbb{C} \mid -1/2 \le x \le 1/2,\ |z| \ge 1\}.$$

This is an example of a *closed fundamental domain,* meaning that it tessellates the upper half-plane, $\mathbb{H} = \Gamma\mathcal{F}$, and different copies overlap only on the boundary, i.e. $V\mathcal{F}^\circ \cap W\mathcal{F}^\circ = \emptyset$ if $V \neq W \in \Gamma$. By the covering property it is clear that for any $z \in \mathbb{H}$ there exists some $A \in \Gamma$ such that $Az \in \mathcal{F}$ and it is easy to see that unless $z$ is equivalent to a point on the boundary of $\mathcal{F}$ this element $A$ is unique. This geometric reduction can then be translated into a reduction theory of, for instance, binary quadratic forms, by noting that the action of $\Gamma$ on $q(x, y) = ax^2 + bxy + cy^2$ with discriminant $\Delta = b^2 - 4ac < 0$ is equivalent to the action of $\Gamma$ on the point $x_0 = \frac{1}{2a}(-b + i\sqrt{|\Delta|})$ in the upper half-plane.

The goal and raison d'être of the current paper is to present, for the first time, an explicit reduction algorithm for Hilbert modular groups which applies to any totally real number field and can be proven to return a reduced point and terminates in polynomially bounded time for a fixed field. With notation as in the following sections our main result is the following.

**Theorem 1.** *Given a totally real number field $K$ and $\mathbf{z} = \mathbf{x} + i\mathbf{y} \in \mathbb{H}_K$ there exists an explicit algorithm (Algorithm 12), which finds an element $A \in \Gamma_K$ such that $A\mathbf{z} \in \mathcal{F}_K$, where $\mathcal{F}_K$ is a certain fundamental domain for $\Gamma_K$. Furthermore, the runtime of this algorithm is polynomial in $\mathrm{N}(\mathbf{x})$, $\mathrm{N}(\mathbf{y})$, $\mathrm{N}\left(\mathbf{y}^{-1}\right)$ as $\mathbf{z}$ varies.*

We will follow a construction of fundamental domains for Hilbert modular groups that originated with Blumenthal [1] and was further improved by e.g. Maaß [15], Herrmann [12] and Tamagawa [21]. A comprehensive description of this method is given in the lecture notes by Siegel [17, Ch. 3.2] and it is this presentation we have mainly followed.

The fundamental domains for quadratic fields and in particular $\mathbb{Q}(\sqrt{5})$ and some others of class number one have been studied in more detail both theoretically and numerically by e.g. Götzky [9], Cohn [3,4], Deutsch [6,7], Jespers, Kiefer and del Río [13], and Quinn and Verjovsky [16].

The intention with the presentation of this paper is to make sure that the exposition is as self-contained as possible and that all details and notations are clear to the reader, in particular, regarding which groups we consider. The following three sections, 2, 3 and 4, are therefore mainly aiming at reformulating elementary results from mainly Siegel [17, Ch. 3.2] and van der Geer [23] but also other sources, into a common language. We start with a brief summary of number fields and embeddings, followed by a section on Hilbert

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

ARTICLE IN PRESS



modular groups and the different types of elements. After this we give a theoretical presentation of the fundamental domain and the different components involved. This is followed by Section 5, where a detailed analysis of the proof of the existence of a closest cusp gives rise to Theorem 5, which is the theoretical foundation behind the algorithm.

After all necessary theoretical results are presented we then give the actual reduction Algorithm, separated in two algorithms to be more comprehensive. After this we provide a selection of detailed examples with the aim to demonstrate the veracity and effectiveness of the algorithm, covering examples of class number greater than one and degree greater than two, both of which previous numerical methods have not been able to deal with successfully. As a conclusion we mention some proposed further work and applications.

It should be noted that all algorithms mentioned in this paper are implemented using SageMath [22] and are available as a Python package at [20]. Furthermore, all examples presented in Section 7 (and more) are available in Jupyter notebook format as part of this package.

*Motivation and future applications*

Our interest in reduction theory for Hilbert modular groups stems from two different problems. The first problem is regarding dimension formulas for vector-valued Hilbert modular forms. This is part of ongoing work joint with Skoruppa and Boylan, cf. e.g. [18] and [19]. One of the necessary ingredients for dimension formulas is the number of elliptic fixed points, and in the vector-valued case it is also necessary to know the corresponding stabilizers. The number of elliptic fixed points is well known for quadratic fields but for higher degrees this is a hard problem for which a computational approach currently seems to be the only option. While there are many computational approaches, both algebraic and analytic, at some point they generally require some form of reduction to produce representative elements.

The second problem is the computation of non-holomorphic Hilbert modular forms. One of the key ingredients in the so-called automorphy (or Hejhal's) method for computing Maaßcusp forms on Hecke triangle groups and subgroups of the modular groups is the existence of an efficient reduction algorithm. Cf. e.g. [11]. While many parts of this algorithm need to be modified to work over fields other than $\mathbb{Q}$, the main obstacle so far has been the lack of a general reduction algorithm. With the existence of the current algorithm the hope is that a computational approach to non-holomorphic Hilbert modular forms is finally within reach.

From an algorithmic perspective it is clear the most important improvement would be to find a better bound for the embeddings or norms in Theorem 5. While we believe that most of the bounds are close to optimal in the general setting it might be possible to hard-code the case of, say, a quadratic field, more efficiently.

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

## 2. Number fields and embeddings

Let $K$ be a totally real number field of degree $n$ over $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$ and unit group $\mathcal{U}$. Choose an integral basis $\alpha_1, \ldots, \alpha_n$ of $\mathcal{O}_K$ and a set of generators (fundamental units) $\varepsilon_1, \ldots, \varepsilon_{n-1}$ of $\mathcal{U}$. Let $\varphi_i : K \hookrightarrow \mathbb{R}$, $i = 1, \ldots, n$ be the embeddings of $K$ into $\mathbb{R}$ and define the norm and trace on $K/\mathbb{Q}$ by

$$\mathrm{N} \coloneqq \mathrm{N}_{K/\mathbb{Q}} : \alpha \mapsto \prod \varphi_i(\alpha) \quad \text{and} \quad \mathrm{Tr} \coloneqq \mathrm{Tr}_{K/\mathbb{Q}} : \alpha \mapsto \sum \varphi_i(\alpha).$$

When there is no risk of confusion we sometimes write $\alpha_i$ for $\varphi_i(\alpha)$. The ideal class number of $K$ is denoted by $h$ and we let $\mathfrak{c}_1, \ldots, \mathfrak{c}_h$ be the set of ideal classes, with $\mathfrak{c}_1$ the trivial class, and $\mathfrak{a}_1 = (1), \mathfrak{a}_2, \ldots, \mathfrak{a}_h$ a fixed set of ideal class representatives, chosen by selecting a fixed ideal of smallest norm in each class.

An element $\alpha \in K$ is said to be totally positive, and we write $\alpha \gg 0$, if $\varphi_i(\alpha) > 0$ for all embeddings $\varphi_i$. To further simplify certain formulas we introduce the rings $\mathbb{C}_K = \mathbb{C} \otimes_{\mathbb{Q}} K$ and $\mathbb{R}_K = \mathbb{R} \otimes_{\mathbb{Q}} K$ and view $\mathbb{C}_K$ as an algebra over both $\mathbb{C}$ and $K$ with the multiplication operations defined in the natural way. More precisely, for pure tensors $\mathbf{z}, \mathbf{z}' \in \mathbb{C}_K$ with $\mathbf{z} = z \otimes a$ and $\mathbf{z}' = z' \otimes a'$ for some $z, z' \in \mathbb{C}$ and $a, a' \in K$ we define

$$\mathbf{z}\mathbf{z}' = zz' \otimes aa', \quad z'\mathbf{z} = \mathbf{z}z' = (z'z) \otimes a, \quad a'\mathbf{z} = \mathbf{z}a' = z \otimes (a'a),$$

and then extend these operations to the whole of $\mathbb{C}_K$ by linearity, and similarly for elements of $\mathbb{R}_K$. The real and imaginary parts of $\mathbf{z} = z \otimes a$ are defined by

$$\Im(\mathbf{z}) = \Im(z) \otimes a \in \mathbb{R}_K \quad \text{and} \quad \Re(\mathbf{z}) = \Re(z) \otimes a \in \mathbb{R}_K,$$

again extended linearly, and we will write a general $\mathbf{z} \in \mathbb{C}_K$ as $\mathbf{z} = \mathbf{x} + i\mathbf{y}$ with $\mathbf{x} = \Re(\mathbf{z})$ and $\mathbf{y} = \Im(\mathbf{z})$. The embeddings $\varphi_i$ are extended to embeddings of $\mathbb{C}_K$ in $\mathbb{C}$ and $\mathbb{R}_K$ in $\mathbb{R}$, respectively, by setting

$$\varphi_i(\mathbf{z}) = \varphi_i(z \otimes a) = z\varphi_i(a)$$

and we use these to define the trace and norm on $\mathbb{C}_K$ and $\mathbb{R}_K$. An element $\mathbf{x} \in \mathbb{R}_K$ is said to be totally positive, written $\mathbf{x} \gg 0$, if $\varphi_i(\mathbf{x}) > 0$ for all embeddings $\varphi_i$ and similarly we write $\mathbf{x} \gg \mathbf{y}$, or equivalently, $\mathbf{y} \ll \mathbf{x}$, if $\mathbf{x} - \mathbf{y} \gg 0$. If $\mathbf{z} \in \mathbb{C}_K$ then $|\mathbf{z}| \in \mathbb{R}_K$ is defined by $\varphi_i(|\mathbf{z}|) = |\varphi_i(\mathbf{z})|$ for all $i$. We define an analog of the standard upper half-plane by setting

$$\mathbb{H}_K = \{\mathbf{z} \in \mathbb{C}_K \mid \Im(\mathbf{z}) \gg 0\}.$$

Many classical results about Hilbert modular groups and forms are formulated in terms of $n$ copies of the standard upper half-plane

$$\mathbb{H}^n = \{(z_1, \ldots, z_n) \in \mathbb{C}^n \mid \Im(z_i) > 0,\, 1 \le i \le n\}$$

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

ARTICLE IN PRESS



but it is very easy to translate results between this and $\mathbb{H}_K$ using the embedding $\varphi$ of $\mathbb{C}_K$ into $\mathbb{C}^n$ (as vector spaces) given by

$$\mathbf{z} \mapsto \varphi(\mathbf{z}) = (\varphi_1(\mathbf{z}), \ldots, \varphi_n(\mathbf{z})) \in \mathbb{C}^n.$$

## 3. Hilbert modular groups

For the purpose of this paper it is most natural to define the Hilbert modular group for $K$ as the projective group

$$\Gamma_K = \mathrm{PSL}_2(\mathcal{O}_K) \simeq \mathrm{SL}_2(\mathcal{O}_K)/\{\pm I_2\},$$

where $I_2$ is the 2-by-2 identity matrix, and we usually represent the elements of $\Gamma_K$ by the associated matrices. In connection with cusps it is also natural to consider the following group associated with an integral ideal $\mathfrak{b}$ of $K$:

$$\Gamma(\mathcal{O}_K \oplus \mathfrak{b}) = \left\{ \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right), \alpha, \delta \in \mathcal{O}_K, \beta \in \mathfrak{b}^{-1}, \gamma \in \mathfrak{b}, \alpha\delta - \beta\gamma = 1 \right\} \subseteq \mathrm{PSL}_2(K).$$

The group $\mathrm{PSL}_2(K)$ acts on $\mathbb{H}_K$ by linear fractional transformations:

$$A(\mathbf{z}) = \frac{\alpha\mathbf{z} + \beta}{\gamma\mathbf{z} + \delta} := (\alpha\mathbf{z} + \beta)(\gamma\mathbf{z} + \delta)^{-1} \quad \text{if } A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{PSL}_2(K), \tag{3.1}$$

and this action is extended as usual to $\mathbb{P}^1(K)$ by setting

$$A(\rho : \sigma) = (\alpha\rho + \beta\sigma : \gamma\rho + \delta\sigma) \quad \text{if} \quad (\rho : \sigma) \in \mathbb{P}^1(K). \tag{3.2}$$

Elements of $\mathrm{PSL}_2(K)$ can be classified, for instance, by using the trace of the associated matrix. For convenience we use the same terminology as in $\mathrm{GL}_2(\mathbb{R})$ and we say that $A$ is:

- *parabolic* if $\mathrm{Tr}(A) = \pm 2$,
- *elliptic* if $|\mathrm{Tr}(A)| \ll 2$, and
- *hyperbolic* if $|\mathrm{Tr}(A)| \gg 2$.

It is clear that $A$ is elliptic, parabolic or hyperbolic precisely if all embeddings $\varphi_i(A)$ are of the corresponding type in $\mathrm{GL}_2(\mathbb{R})$. An element that does not belong to any of these types is simply said to be *mixed*. It is not hard to show that $A$ is parabolic if and only if it has a unique fixed point in $\mathbb{P}^1(K)$, elliptic if and only if it has a unique fixed point in $\mathbb{H}_K$ and hyperbolic if and only if it has two fixed points in $\mathbb{P}^1(K)$. For more details see e.g. Freitag [8, II.§2-§3].

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

ARTICLE IN PRESS



### 3.1. Element and generators of the Hilbert modular group

If $\alpha \in \mathcal{O}_K$ and $\varepsilon \in \mathcal{U}$ we define the following elements of $\Gamma_K$:

$$T^\alpha := \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \quad E(\varepsilon) := \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} \quad \text{and } S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

and note that the corresponding actions on $\mathbb{H}_K$ are given by the maps

$$T^\alpha : \mathbf{z} \mapsto \mathbf{z} + \alpha, \quad E(\varepsilon) : \mathbf{z} \to \varepsilon^2 \mathbf{z} \quad \text{and } S : \mathbf{z} \to -\mathbf{z}^{-1}.$$

For an integral ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ we define the *translation module* of $\mathfrak{a}$ by

$$\mathbb{T}^{\mathfrak{a}} := \left\{ T^\beta \mid \beta \in \mathfrak{a} \right\}$$

and if $\mathcal{H} \leqslant \mathcal{U}$ is generated by $\varepsilon_1^{a_1}, \varepsilon_2^{a_2}, \dots, \varepsilon_{n-1}^{a_{n-1}}$ then the set of *multipliers* of $\mathcal{H}$ is

$$\mathbb{M}_{\mathcal{H}} := \{ E(\varepsilon) \mid \varepsilon \in \mathcal{H} \} \simeq \langle E(\varepsilon_1^{a_1}) \rangle \times \cdots \times \left\langle E(\varepsilon_{n-1}^{a_{n-1}}) \right\rangle.$$

Let $\beta_1, \dots, \beta_n$ and $\beta_1', \dots, \beta_n'$ be integral bases of $\mathfrak{a}$ and $\mathfrak{a}^{-1}$. It is clear that the translation modules are finitely generated, more precisely

$$\mathbb{T}^{\mathfrak{a}} \simeq \left\langle T^{\beta_1} \right\rangle \times \cdots \times \left\langle T^{\beta_n} \right\rangle \quad \text{and} \quad \mathbb{T}^{\mathfrak{a}^{-1}} \simeq \left\langle T^{\beta_1'} \right\rangle \times \cdots \times \left\langle T^{\beta_n'} \right\rangle.$$

It follows by a result of Vaseršteĭn [24] (see also [14] and [23, p. 82]) that $\Gamma(\mathcal{O}_K \oplus \mathfrak{a})$ is generated by upper and lower-triangular matrices and since these can all be expressed in terms of the elements $S$ and $T^\alpha$ it is generated by the set

$$\{S, T^{\beta_1}, T^{\beta_2}, \dots, T^{\beta_n}, T^{\beta_1'}, \dots, T^{\beta_n'}\}.$$

As a special case we conclude that $\Gamma_K = \Gamma(\mathcal{O}_K \oplus \mathcal{O}_K)$ is generated by $\{S, T^{\alpha_1}, \dots, T^{\alpha_n}\}$. This set of generators is very simple and an immediate extension of the well-known generators $S$ and $T = T^1$ for $\mathrm{PSL}_2(\mathbb{Z})$. Unfortunately, in the case of $\Gamma_K$, these generators do not have the same geometric significance and in particular do not correspond to side-pairing transformations. They are therefore not immediately useful in a reduction algorithm. It is therefore common to consider a slightly larger set of generators including elements $E(\varepsilon)$ with $\varepsilon \in \mathcal{U}$ even though these can of course be expressed by the other generators using, for instance, the algorithms introduced in [10].

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

### 3.2. Cusps of Hilbert modular groups

The set of *cusps* of $\Gamma_K$, in other words, fixed points of parabolic elements, can be identified with the projective line $\mathbb{P}^1(K) = K \cup \{\infty\}$ where the cusp at infinity, $\infty$, is as usual a convenient symbol for the class $(1:0)$. Most results below are well-known and for proofs and further details we refer the reader to e.g. [23] or [5]. Note that $\Delta(\mathcal{O}_K, \mathfrak{b}^{-1})$ in the notation of [5] corresponds to the group $\Gamma(\mathcal{O}_K \oplus \mathfrak{b})$ in our notation.

Every cusp $\lambda \in \mathbb{P}^1(K)$ can be represented by $(\rho : \sigma)$ for some non-unique pair $\rho, \sigma \in \mathcal{O}_K$ with associated fractional ideal $\mathfrak{a}_{\rho,\sigma} = (\rho, \sigma)$. It is easy to see that different representatives for $\lambda$ give rise to fractional ideals in the same ideal class, denoted by $\mathfrak{c}_\lambda \in \mathrm{Cl}(K)$. For any $\lambda \in \mathbb{P}^1(K)$ we assume that $\rho$ and $\sigma$ are chosen such that $(\rho, \sigma) = \mathfrak{a}_j$ for some ideal class representative $\mathfrak{a}_j$.

Furthermore, the ideals associated with $(\rho : \sigma)$ and $A\,(\rho : \sigma)$ are identical if $A \in \Gamma_K$ since $\det(A) = 1$. It can be shown that the map $\lambda \mapsto \mathfrak{c}_\lambda$ is a bijection from $\Gamma_K \backslash \mathbb{P}^1(K) \to \mathrm{Cl}(K)$ and therefore the number of $\Gamma_K$-equivalence classes of cusps is equal to $h$, the ideal class number of $K$, and we choose $\lambda_1 = \infty, \ldots, \lambda_h$ as representatives for $\Gamma \backslash \mathbb{P}^1(K)$ such that $\lambda_j$ is associated with $\mathfrak{c}_j$ and we write $\lambda_j = (\rho_j : \sigma_j)$ with $(\rho_j, \sigma_j) = \mathfrak{a}_j$.

It is easy to see that the stabilizer of the cusp $\infty$ in $\Gamma_K$ is given by

$$\Gamma_{K,\infty} := \left\{ T^\alpha E(\varepsilon) = \left(\begin{smallmatrix} \varepsilon & \varepsilon^{-1}\alpha \\ 0 & \varepsilon^{-1} \end{smallmatrix}\right) : \mathbf{z} \mapsto \varepsilon^2 \mathbf{z} + \alpha,\ \varepsilon \in \mathcal{U},\ \alpha \in \mathcal{O}_K \right\} \simeq T^{\mathcal{O}_K} \rtimes \mathcal{U}^2.$$

Corresponding to each cusp representative $\lambda_j = (\rho_j : \sigma_j)$ we choose a cusp normalizing map, $A_j \in \mathrm{PGL}_2(\mathcal{O}_K)$, such that $A_j\,(\infty) = \lambda_j$ and

$$A_j = \begin{pmatrix} \rho_j & \xi_j \\ \sigma_j & \eta_j \end{pmatrix}$$

with $\xi_j, \eta_j \in \mathfrak{a}_j^{-1}$ and $\rho_j \eta_j - \sigma_j \xi_j = 1$. In the notation of [5] $A_j$ is an $(\mathfrak{a}_j, \mathfrak{a}_j^{-1})$-matrix. The map $A_j$ is unique up to multiplication by an element in $\Gamma_{K,\infty}$ on the right and we have

$$A_j^{-1} \Gamma_K A_j = \Gamma(\mathcal{O}_K \oplus \mathfrak{a}_j^2).$$

As an alternative to studying the set of cusp representatives $\lambda_1, \ldots, \lambda_h$ of $\Gamma_K$ it is therefore possible to consider the cusp at $\infty$ for the collection of groups $\Gamma\left(\mathcal{O}_K \oplus \mathfrak{a}_j^2\right)$ for $j = 1, \ldots, h$, with stabilizers

$$\begin{aligned} \Gamma(\mathcal{O}_K \oplus \mathfrak{a}_j^2)_\infty &= \left\{ T^\alpha E(\varepsilon) = \left(\begin{smallmatrix} \varepsilon & \varepsilon^{-1}\alpha \\ 0 & \varepsilon^{-1} \end{smallmatrix}\right) : \mathbf{z} \mapsto \varepsilon^2 \mathbf{z} + \alpha,\ \varepsilon \in \mathcal{U},\ \alpha \in \mathfrak{a}_j^{-2} \right\} \\ &\simeq T^{\mathfrak{a}_j^{-2}} \rtimes \mathcal{U}^2. \end{aligned}$$

For an arbitrary cusp $\mu \in \mathbb{P}^1(K)$ we choose a map $U_\mu \in \Gamma_K$ such that $U_\mu\,(\mu) = \lambda_{I(\mu)}$ where $I(\mu)$ is a unique integer in $\{1, 2, \ldots, h\}$ and define the cusp normalizer of $\mu$ as

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

ARTICLE IN PRESS



$$A_\mu = U_\mu^{-1} A_{I(\mu)}.$$

It is now easy to show (see e.g. [17]) that the stabilizer of an arbitrary cusp $\mu \in K$ in $\Gamma_K$ can be written as

$$\Gamma_{K,\mu} = A_\mu \Gamma(\mathcal{O}_K \oplus \mathfrak{a}_{I(\mu)}^2)_\infty A_\mu^{-1}$$

where $\mathfrak{a}_{I(\mu)}$ is the ideal corresponding to the cusp representative $\lambda_{I(\mu)}$ which is equivalent to $\mu$. In particular, all elements that stabilizes $\mu$ in $\Gamma_K$ can be written as $A_\mu T^\alpha E(\varepsilon) A_\mu^{-1}$ for some $\varepsilon \in \mathcal{U}$ and $\alpha \in \mathfrak{a}_{I(\mu)}^{-2}$.

## 4. The fundamental domain

The fundamental domain we describe in this section is essentially the same as that used by Bluhmenthal [1], Mass [15], Tamagawa [21], Siegel [17] and others. The main difference in these authors' approaches is in the description of the "bottom" part which consists of a collection of hypersurfaces. Here we adopt the description given by Siegel [17] since it is easy to use for the explicit reduction algorithm. We have aimed to provide sufficient details to demonstrate the appropriateness and correctness of the algorithm and refer to [17] for details and proofs.

### *4.1. Reduction with respect to units*

We use $\log : \mathbb{R}^+ \to \mathbb{R}$ to denote the natural logarithm and without risk of confusion we use the same notation for the extended map $\log : \mathbb{R}_K^+ \to \mathbb{R}^n$ defined by $\log(\mathbf{x}) = (\log \varphi_1(\mathbf{x}), \ldots, \log \varphi_n(\mathbf{x}))$. It is immediate from Dirichlet's unit theorem that the group of units squared, $\mathcal{U}^2$, corresponds to an integral lattice $\Lambda$ of rank $n-1$ in $\mathbb{R}^n$, explicitly given by:

$$\Lambda = \log(\mathcal{U}^2) = \left\{\log(\varepsilon) \,:\, \varepsilon \in \mathcal{U}^2\right\} = \left\{\sum_{k=1}^{n-1} a_k \log(|\varepsilon_k|) \,:\, a_k \in 2\mathbb{Z}\right\}.$$

The vectors $\log|\varepsilon_k| = (\log|\varphi_1\varepsilon_k|, \ldots, \log|\varphi_n\varepsilon_k|)^t$ form a basis of $\Lambda$ and we let $B_\Lambda = (b_{rk})_{1\le r\le n, 1\le k\le n-1} \in M_{n\times n-1}(\mathbb{R})$ with $b_{rk} = \log|\varphi_r(\varepsilon_k)|$ denote the corresponding basis matrix. Since all units have norm 1 it is easy to see that $\Lambda$ is contained in the $n-1$-dimensional hyperplane

$$H = \{\mathbf{u} \in \mathbb{R}^n \mid u_1 + \ldots + u_n = 0\}.$$

We follow the explicit construction by Siegel and choose $K_\Lambda = B_\Lambda[-1, 1[^{n-1}$ as a fundamental parallelepiped for $\Lambda$ and say that a vector in $H$ is $\Lambda$-reduced if it belongs to $K_\Lambda$. If $\mathbf{y} \in \mathbb{R}_K^+$ we define $\tilde{\mathbf{y}} = \mathbf{y} \cdot (\mathrm{N}\mathbf{y})^{-1/n}$ and observe that $\mathrm{N}\tilde{\mathbf{y}} = 1$, hence $\log(\tilde{\mathbf{y}}) \in H$ and we say that $\mathbf{y}$ is $\mathcal{U}^2$-reduced if $\log(\tilde{\mathbf{y}})$ is $\Lambda$-reduced. This means that we can write

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

$$B_\Lambda \mathbf{Y} = \log(\tilde{\mathbf{y}}), \tag{4.1}$$

where $\mathbf{Y} \in [-1,1[^{n-1}$. The complete coordinate map $\mathbf{Y}_\Lambda : \mathbb{R}_K^+ \to [-1,1[^{n-1}$ is then defined by setting $\mathbf{Y}_\Lambda(\mathbf{y}) = \mathbf{Y}$ where $\mathbf{Y}$ satisfies (4.1). Observe that if $\mathbf{b} = (b_1, \ldots, b_{n-1})^t \in \mathbb{Z}^{n-1}$ then

$$B_\Lambda \mathbf{b} = \sum_{k=1}^{n-1} b_k \log|\varepsilon_k|$$

and therefore, if $\varepsilon = \varepsilon_1^{b_1} \cdots \varepsilon_{n-1}^{b_{n-1}} \in \mathcal{U}$ then $\mathbf{Y}_\Lambda(\varepsilon^2 \mathbf{y}) = \mathbf{Y}_\Lambda(\mathbf{y}) + 2\mathbf{b}$. It follows that if we are given a $\mathbf{y} \in \mathbb{R}_K^+$ with $\mathbf{Y}_\Lambda(\mathbf{y}) = (Y_1, \ldots, Y_{n-1})$ and choose $b_i = -\left\lfloor \frac{Y_i}{2} + \frac{1}{2} \right\rfloor$ then $E(\varepsilon)\mathbf{y} = \varepsilon^2 \mathbf{y}$ will be $\mathcal{U}^2$ reduced. Here $\lfloor x \rfloor$ is the nearest integer to $x$, defined as the unique integer $n$ satisfying $x - 1/2 \leq n < x + 1/2$.

It is easy to see that $K_\Lambda \simeq \Lambda \backslash \mathbb{R}^{n-1}$ is isomorphic via the logarithm map to a fundamental domain for the action of the set of multipliers $\mathbb{M}_{\mathcal{U}}$ on $\mathbb{R}_K^+$. For the explicit computations of reduced vectors it is useful to have the following explicit estimates in terms of the absolute row sums of $B_\Lambda$:

$$r_i(B_\Lambda) = \sum_{j=1}^{n-1} \left| \log|\varphi_i \varepsilon_j| \right|, \quad 1 \leq i \leq n,$$

and we observe that $\|B_\Lambda\|_\infty = \max r_i(B_\Lambda)$.

**Lemma 2.** *If $\mathbf{u} \in \mathbb{R}^n$ is $\Lambda$-reduced then $|u_i| \leq r_i(B_\Lambda)$.*

**Proof.** If $\mathbf{u} \in K_\Lambda$ then $\mathbf{u} = B_\Lambda \mathbf{Y}$ for some $\mathbf{Y} \in [-1,1]^{n-1}$ and hence

$$|u_i| = (B_\Lambda \mathbf{Y})_i \leq \sum_{j=1}^{n-1} \left| \log|\varphi_i \varepsilon_j| \right| |Y_j| \leq r_i(B_\Lambda). \quad \square$$

The following corollary is now immediate.

**Corollary 3.** *If $\mathbf{y} \in \mathbb{R}_K^+$ then there is a unit $\varepsilon \in \mathcal{U}^2$ such that*

$$(\mathrm{N}\mathbf{y})^{1/n} e^{-r_i(B_\Lambda)} \leq |\varphi_i(\varepsilon \mathbf{y})| \leq (\mathrm{N}\mathbf{y})^{1/n} e^{r_i(B_\Lambda)} \quad \textit{for all } 1 \leq i \leq n.$$

## *4.2. Reduction with respect to translations*

Let $\mathfrak{a}$ be an integral ideal in $\mathcal{O}_K$ and choose an integral basis $\beta_1^{(\mathfrak{a})}, \ldots, \beta_n^{(\mathfrak{a})}$ of $\mathfrak{a}$. Using the embedding map we identify $\mathfrak{a}$ with a lattice of rank $n$ in $\mathbb{R}^n$, also denoted by $\mathfrak{a}$. The basis matrix for this lattice is denoted by $B_\mathfrak{a}$ and we choose a fundamental polytope $K_\mathfrak{a} = B_\mathfrak{a}[-1/2, 1/2[^n$. For an element $\mathbf{x} \in \mathbb{R}_K$ we define the $\mathfrak{a}$-coordinate vector $\mathbf{X}_\mathfrak{a}(\mathbf{x})$ by the equation

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

$$B_{\mathfrak{a}}\mathbf{X}_{\mathfrak{a}}(\mathbf{x}) = \varphi(\mathbf{x})$$

and say that $\mathbf{x}$ is $\mathfrak{a}$-reduced if $\varphi(\mathbf{x}) \in K_{\mathfrak{a}}$, or in other words, if $\mathbf{X}_{\mathfrak{a}}(\mathbf{x}) = (X_1, \ldots, X_n)$ with $-1/2 \leq X_k < 1/2$ for all $k$s.

If $\alpha = \sum_{k=1}^{n} a_k \beta_k^{(\mathfrak{a})} \in \mathfrak{a}$ then $\mathbf{X}_{\mathfrak{a}}(\alpha) = (a_1, \ldots, a_n)$ and it is clear that $\mathbf{X}_{\mathfrak{a}}(\mathbf{x} + \alpha) = (X_1 + a_1, \ldots, X_n + a_n)$ and hence, if we choose $a_k = -\lfloor X_k \rfloor$ then $T^{\alpha}\mathbf{x} = \mathbf{x} + \alpha$ will be $\mathfrak{a}$-reduced.

### 4.3. Fundamental domain for the cusp stabilizer

Let $\lambda \in \mathbb{P}^1(K)$ be a cusp of $\Gamma_K$, $\mathfrak{a}_\lambda$ the corresponding representative ideal and $\mathfrak{b} = \mathfrak{a}_\lambda^{-2}$ with an integral basis $\beta_1^{(\mathfrak{b})}, \ldots, \beta_n^{(\mathfrak{b})}$. For an element $\mathbf{z} \in \mathbb{H}_K$ we define $\mathbf{z}_\lambda = \mathbf{x}_\lambda + i\mathbf{y}_\lambda = A_\lambda^{-1}\mathbf{z}$ and say that $\mathbf{z}$ is reduced with respect to $\lambda$ if $\mathbf{x}_\lambda$ is reduced with respect to $\mathfrak{b}$ and $\mathbf{y}_\lambda$ is reduced with respect to $\mathcal{U}^2$. We let $\mathcal{C}_\lambda$ denote the set of all such reduced points, more precisely

$$\mathcal{C}_\lambda = \left\{\mathbf{z} \in \mathbb{H}_K \mid \mathbf{X}_{\mathfrak{b}}(\mathbf{x}_\lambda) \in [-1/2, 1/2[^n \text{ and } \mathbf{Y}_\Lambda(\mathbf{y}_\lambda) \in [-1, 1[^{n-1}\right\}.$$

It is easy to show that the set $\mathcal{C}_\lambda$ is indeed a fundamental domain for the action of $\Gamma_{K,\lambda} = A_\lambda \Gamma(\mathcal{O}_K \oplus \mathfrak{a}_\lambda^2) A_\lambda^{-1}$ on $\mathbb{H}_K$. Note that for the modular group, $\mathrm{PSL}_2(\mathbb{Z})$, the analogue of the domain $\mathcal{C}_\lambda$ is the strip $-1/2 < \Re(z) \leq 1/2$.

### 4.4. Cuspidal regions

If the regions $\mathcal{C}_\lambda$ in the previous section are analogues of the vertical strip we will now look at the analog of the curved part of the fundamental domain, given by $|z| \geq 1$. For the modular group this can be interpreted in terms of a reflection in the isometric circle corresponding to the map given by $z \mapsto -z^{-1}$. An analog interpretation is valid for Hilbert modular groups but it is much harder to work out precisely which reflections to include even for small number fields of class number 1.

If $\mathbf{z} = \mathbf{x} + i\mathbf{y} \in \mathbb{H}_K$ we define $\Delta(\mathbf{z}, \infty)$, the *distance* to the cusp at $\infty$, by

$$\Delta(\mathbf{z}, \infty) = \mathrm{N}\left(\Im \mathbf{z}\right)^{-1/2}$$

and the distance to an arbitrary cusp $\mu = (\rho : \sigma)$ with associated ideal $\mathfrak{a} = (\rho, \sigma)$ is

$$\begin{aligned}\Delta(\mathbf{z}, \mu) &= \mathrm{N}\left(\mathfrak{a}\right)^{-1} \mathrm{N}(\Im A_\mu^{-1}\mathbf{z})^{-1/2} = \mathrm{N}\left(\mathfrak{a}\right)^{-1} \mathrm{N}\left(\mathbf{y}\right)^{-1/2} \mathrm{N}(\left|-\sigma\mathbf{z} + \rho\right|^2)^{1/2} \qquad (4.2)\\ &= \mathrm{N}(\mathfrak{a})^{-1}\mathrm{N}\left(\left(-\sigma\mathbf{x} + \rho\right)^2 \mathbf{y}^{-1} + \sigma^2\mathbf{y}\right)^{\frac{1}{2}},\end{aligned}$$

where $\mathrm{N}(\mathfrak{a})$ is the norm of the ideal $\mathfrak{a}$. This expression is independent of the choice of representatives $\rho$ and $\sigma$ as well as the choice of $A_\mu$. Observe that the normalization factor $N(\mathfrak{a})^{-1}$, which accounts for the independence of the choices of $\rho$ and $\sigma$ is present in [23]

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

ARTICLE IN PRESS



but not in [17]. The expression $\Delta(\mathbf{z},\mu)$ is in fact bi-invariant under $\Gamma_K$, in other words, $\Delta(A\mathbf{z},A\mu) = \Delta(\mathbf{z},\mu)$ for all $A \in \Gamma_K$. We will show later, in Lemma 4, that for every $\mathbf{z} \in \mathbb{H}_K$ there exists a cusp $\lambda$ which is closest to $\mathbf{z}$ and it follows that the *invariant height*

$$\Delta(\mathbf{z}) = \inf\left\{\Delta(\mathbf{z},\lambda) \mid \lambda \in \mathbb{P}^1(K)\right\}$$

is well-defined, invariant under $\Gamma_K$ and $\Delta(\mathbf{z}) = \Delta(\mathbf{z},\lambda)$ for some cusp $\lambda$ (not necessarily unique).

We are now fully prepared to give the definition of the fundamental domain that we are interested in. For a cusp representative $\lambda_j$ with $1 \le j \le h$ we let $\mathcal{F}_j$ denote the set of $\lambda_j$-reduced points that are closest to $\lambda_j$, in other words:

$$\mathcal{F}_j = \left\{\mathbf{z} \in \mathcal{C}_{\lambda_j} \mid \Delta(\mathbf{z}) = \Delta(\mathbf{z},\lambda_j)\right\}.$$

It can then be shown (cf. e.g. [17]) that the set

$$\mathcal{F}_K = \cup_{j=1}^{h} \mathcal{F}_j$$

is a fundamental domain for the action of $\Gamma_K$ on $\mathbb{H}_K$. Given that $\mathcal{F}_K$ is a fundamental domain we now turn to the problem of reducing a point $\mathbf{z}$ to its representative inside $\mathcal{F}_K$. It is clear that the as soon as we find a closest cusp, say $\mu \in \mathbb{P}^1(K)$, which is equivalent to a cusp representative $\lambda_j$ with $U_\mu(\mu) = \lambda_j$ then $\lambda_j$ is a closest cusp to $U_\mu \mathbf{z}$ and we can use the straight-forward reduction with respect to units and translations from Sections 4.1 and 4.2 to find an $\varepsilon \in \mathcal{U}^2$ and $\alpha \in \mathfrak{a}_j^{-2}$ such that $\mathbf{z}^* = A_{\lambda_j} T^{\alpha} E(\varepsilon) A_{\lambda_j}^{-1} U_\mu \mathbf{z}$ belongs to $\mathcal{F}_j$.

The reduction with respect to units and translations is essentially done in constant time independent of $\mathbf{z}$ and has been efficiently implemented by many authors, cf. e.g. [2]. The practical and theoretical complexity of the reduction algorithm is almost entirely in the finding of the closest cusp. The next section is dedicated to auxiliary results and details on how our algorithm for finding the closest cusp works and we will then summarize the actual algorithm in the following section.

## 5. Finding the closest cusp

Our approach to finding the closest cusp $\lambda$ is to analyze the existence and conditional uniqueness proofs from the lecture notes of Siegel [17] and find explicit and efficient bounds for all constants involved. The general idea was already present in a slightly different form in the work of Maaß [15] but note that some of the explicit constants present, in e.g. Hilfssatz II, are in general weaker than those we obtain here. The aim of this section is to include sufficient details in the proofs for a reader to be able to both understand and verify the functionality of the associated code [20] as well as being able to implement these algorithms independently.

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

ARTICLE IN PRESS



**Lemma 4.** *If $\mathbf{z} \in \mathbb{H}_K$ then there exists a cusp $\lambda \in \mathbb{P}^1(K)$ such that*

$$\Delta(\mathbf{z}, \lambda) \leq \Delta(\mathbf{z}, \mu) \quad \forall \mu \in \mathbb{P}^1(K).$$

**Proof.** Let $\mathbf{z} = \mathbf{x} + i\mathbf{y} \in \mathbb{H}_K$ be fixed. It is sufficient to show that for any given cusp $\mu$ there exists only a finite number of cusps $\lambda$ such that $\Delta(\mathbf{z}, \lambda) \leq \Delta(\mathbf{z}, \mu)$.

It follows from Section 3.2 that we can assume that $\lambda = (\rho : \sigma)$ where $\rho$ and $\sigma$ are chosen such that $(\rho, \sigma) = \mathfrak{a}_i$ for some class group representative $\mathfrak{a}_i$ and in particular $\mathrm{N}((\rho, \sigma)) \leq C$ where

$$C = \max \{\mathrm{N}(\mathfrak{a}_1), \ldots, \mathrm{N}(\mathfrak{a}_h)\}.$$

We now consider $\Delta(\mathbf{z}, \lambda)$ as a function of the algebraic integers $\sigma$ and $\rho$ and write

$$\Delta_{\mathbf{z}}(\rho, \sigma) := \Delta(\mathbf{z}, (\rho : \sigma)) = \mathrm{N}((\rho, \sigma))^{-1} \left( \mathrm{N} \left( (-\sigma\mathbf{x} + \rho)^2 \mathbf{y}^{-1} + \sigma^2 \mathbf{y} \right) \right)^{\frac{1}{2}}.$$

It is sufficient to show that if $d > 0$ there exists only a finite number of pairs $\rho, \sigma \in \mathcal{O}_K$ modulo units, such that $\Delta_{\mathbf{z}}(\rho, \sigma) < d$. Given such a pair write

$$\Delta_{\mathbf{z}}(\rho, \sigma) = \mathrm{N}((\rho, \sigma))^{-1} (\mathrm{N}\mathbf{w})^{1/2},$$

where $\mathbf{w} = (-\sigma\mathbf{x} + \rho)^2 \mathbf{y}^{-1} + \sigma^2 \mathbf{y} \in \mathbb{R}_K^+$. It follows from Corollary 3 that there exists a unit $\varepsilon \in \mathcal{U}$ such that

$$\left|\varphi_i \left(\varepsilon^2 \mathbf{w}\right)\right| \leq e^{r_i(B_\Lambda)} (\mathrm{N}\mathbf{w})^{\frac{1}{n}} \leq e^{r_i(B_\Lambda)} d^{2/n} C^{2/n}, \quad \text{for all} \quad 1 \leq i \leq n.$$

Setting $\delta_i = e^{r_i(B_\Lambda)} d^{2/n} C^{2/n}$ we can therefore assume that $\sigma$ and $\rho$ have been chosen such that $|\varphi_i(\mathbf{w})| \leq \delta_i$, and hence that

$$\varphi_i(\sigma^2 \mathbf{y}) \leq \delta_i \quad \text{and} \quad \varphi_i((-\sigma\mathbf{x} + \rho)^2 \mathbf{y}^{-1}) \leq \delta_i.$$

It follows that the coordinates of the embeddings of $\sigma$ and $\rho$ are bounded by

$$|\sigma_i|^2 \leq \delta_i y_i^{-1} \quad \text{and} \tag{5.1}$$

$$|\rho_i - \sigma_i x_i|^2 \leq \delta_i y_i. \tag{5.2}$$

The inequalities (5.1) and (5.2) clearly define a bounded domain in $\mathbb{R}^n \times \mathbb{R}^n$ and the statement follows since the embeddings of $\mathcal{O}_K$ form a lattice in $\mathbb{R}^n$. □

An immediate consequence of the previous proof, and in particular (5.1), (5.2) and the inequality $\mathrm{N}(\sigma^2 \mathbf{y}) < \mathrm{N}(\mathbf{w})$, is the following result which is crucial to our algorithm.

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

ARTICLE IN PRESS



**Theorem 5.** *Let $\mathbf{z} \in \mathbb{H}_K$ and assume that there is a cusp $\lambda$ with $\Delta(z, \lambda) = d$. Then a closest cusp can be chosen as $(\rho : \sigma)$ where the embeddings of $\rho$ and $\sigma$ satisfy the following bounds:*

$$|\sigma_i| \leq D_i \cdot d^{1/n} y_i^{-1/2} \quad \text{and} \quad |\rho_i - x_i\sigma_i| \leq D_i \cdot d^{1/n} y_i^{1/2},$$

*where*

$$D_i = C^{1/n} e^{\frac{1}{2} r_i(B_\Lambda)},$$

*and, additionally, the norms are bounded by*

$$\mathrm{N}\left(|\sigma|\right) \leq dC\mathrm{N}\left(\mathbf{y}\right)^{-1/2} \quad \text{and} \quad \mathrm{N}\left(|-\sigma\mathbf{x} + \rho|\right) \leq dC\mathrm{N}\left(\mathbf{y}\right)^{1/2}.$$

To apply the previous theorem we need to find an initial cusp $\lambda$. It is, for instance, always possible to choose $\infty$, in which case $d = \Delta(z, \infty) = \mathrm{N}(\mathbf{y})^{-1/2}$, or 0, in which case $d = \Delta(z, 0) = \mathrm{N}(\mathbf{y})^{-1/2}\mathrm{N}(\mathbf{x}^2 + \mathbf{y}^2)^{1/2}$. However, it is clear that we would like to obtain as small initial bound as possible and if $\mathrm{N}(\mathbf{y})$ is small than we need to find another cusp to start with.

Fortunately there is a method which seems to work well in practice when $\mathrm{N}(\mathbf{y})$ is small. This method was introduced by Bouyer and Streng [2] and the main idea is to use LLL reduction to find a vector of short norm, $-\sigma\mathbf{z} + \rho$, in the lattice $L_{\mathbf{z}} = \mathcal{O}_K\mathbf{z} + \mathcal{O}_K$ and the corresponding cusp $(\rho : \sigma)$ will then be close to $\mathbf{z}$ by (4.2).

**Remark 6.** It should be noted that the LLL reduction method by itself does not necessarily yield the closest cusp, as the LLL algorithm is not guaranteed to return the shortest vector and the definition of distance $\Delta(z, (\rho : \sigma))$ also involves the norm of the ideal $(\rho, \sigma)$. For a provably correct algorithm (in all degrees) it is therefore necessary to combine this preliminary optimization with an exhaustive search using the explicit bounds of Lemma 5.

Since the only integer in $\mathcal{O}_K$ with norm less than 1 is 0 the norm bound of Theorem 5 immediately implies the following.

**Corollary 7.** *Let $\mathbf{z} = \mathbf{x} + i\mathbf{y} \in \mathbb{H}_K$. If $\mathrm{N}(\mathbf{y}) > C$ then $\infty$ is the closest cusp to $\mathbf{z}$.*

Unfortunately it is in general not so easy to find the closest cusp and we will see that it is often necessary to compare distances to many different cusps. However, the number of comparisons needed can sometimes be reduced by using the following Lemma and Corollary.

**Lemma 8.** *There exists a constant $d > 0$, depending only on $K$, such that for all $\mathbf{z} = \mathbf{x} + i\mathbf{y} \in \mathbb{H}_K$, if $\lambda$ and $\mu$ are cusps of $K$ with $\Delta(\lambda, \mathbf{z}) < d$ and $\Delta(\mu, \mathbf{z}) < d$ then $\lambda = \mu$.*

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

**Proof.** Let $\mathbf{z} = \mathbf{x} + i\mathbf{y} \in \mathbb{H}_K$. Assume that $\lambda = (\sigma : \rho)$ and $\mu = (\sigma_1 : \rho_1)$ satisfy $\Delta(\lambda, \mathbf{z}) < d$ and $\Delta(\mu, \mathbf{z}) < d$ for some positive $d$. Observe that the algebraic integer $\rho\sigma_1 - \sigma\rho_1$ can be written

$$\rho\sigma_1 - \sigma\rho_1 = (-\sigma\mathbf{x} + \rho)\,\mathbf{y}^{-1/2}\sigma_1\mathbf{y}^{1/2} - (-\sigma_1\mathbf{x} + \rho_1)\,\mathbf{y}^{-1/2}\sigma\mathbf{y}^{1/2}.$$

Since (5.1) and (5.2) apply to both $(\sigma, \rho)$ and $(\sigma_1, \rho_1)$ it is easy to see that

$$\varphi_i\left(|\rho\sigma_1 - \sigma\rho_1|\right) \leq 2\delta_i,$$

where $\delta_i = e^{r_i(B_\Lambda)}d^{2/n}C^{2/n}$. It follows that $\mathrm{N}\left(\rho\sigma_1 - \sigma\rho_1\right) \leq 2^n \prod \delta_i$ and hence, if $d < C^{-1}2^{-n/2}e^{-\sum r_i(B_\Lambda)}$ then we must have $\rho\sigma_1 - \sigma\rho_1 = 0$ so $\mu = \lambda$. □

**Corollary 9.** *Let $\mathbf{z} = \mathbf{x} + i\mathbf{y} \in \mathbb{H}_K$. If $\lambda$ is a cusp with $\Delta(\lambda, \mathbf{z}) < C^{-1}2^{-n/2}e^{-\sum r_i(B_\Lambda)}$ then $\lambda$ is the closest cusp to $\mathbf{z}$.*

The previous lemma also has the geometric consequence that it is possible to decompose the fundamental domain $\mathcal{F}$ into a compact part and disjoint cuspidal parts.

## 6. Algorithms

We will now describe the actual reduction algorithm in detail. The key idea is to use Theorem 5 to find bounded regions in $\mathbb{R}^n$ where the embeddings of the numerators and denominators of potential closest cusps must be located. We then compare the distance to $\mathbf{z}$ for each of the candidate cusps, except if one of the distances is less than the bound in Corollaries 7 or 9, in which case we terminate the search early.

Recall that we have a fixed integral basis $\alpha_1, \ldots, \alpha_n$ of $\mathcal{O}_K$ and a corresponding lattice in $\mathbb{R}^n$ with basis matrix $B_{\mathcal{O}_K}$. If $\beta \in \mathcal{O}_K$ is given by $\beta = \sum_{i=1}^n X_i\alpha_i$ for some integer vector $\mathbf{X} \in \mathbb{Z}^n$ then the embeddings of $\beta$ correspond to the vector $\varphi(\beta) = B_{\mathcal{O}_K}\mathbf{X}$ in $\mathbb{R}^n$. If we can bound the vector $\varphi(\beta)$ in a parallelotope $P$ it follows that $\mathbf{X}$ must belong to the polytope $B_{\mathcal{O}_K}^{-1}(P)$ and we thus need to find vectors with integer coordinates inside this set.

A preliminary investigation of the performance showed that the most efficient way to find these seems to be to search for integer vectors in a bounding parallelotope of $B_{\mathcal{O}_K}^{-1}(P)$, which we denote by $\mathbb{BP}(B_{\mathcal{O}_K}^{-1}(P))$, and apply the embedding map to test whether or not to include them in the result. Using this idea together with Theorem 5 gives us the following algorithm.

**Algorithm 10** *(Finding the closest cusp). Let $K$ be a fixed totally real number field, all notation be as above and let $\mathbf{z} = \mathbf{x} + i\mathbf{y} \in \mathbb{H}_K$.*

*Step 1: If $\mathrm{N}(\mathbf{y}) > C$ return $\infty = (0 : 1)$ as the closest cusp.*

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

*Step 2: Use the LLL reduction to find a potentially closest cusp, $\lambda$, and set $d = \min\{\Delta(\mathbf{z},\lambda),\Delta(\mathbf{z},\infty),\Delta(\mathbf{z},0)\}$.*

*Step 3: Recall that $C = \max(\mathrm{N}(\mathfrak{a}_1),\dots\mathrm{N}(\mathfrak{a}_h))$ and $D_i = \max C^{1/n}e^{\frac{1}{2}r_i(B_\Lambda)}$. Define*

$$a_i = D_i d^{1/n} y_i^{-1/2},\ 1 \leq i \leq n, \quad \text{and set}$$
$$P_\sigma = [-a_1,a_1]\times\cdots\times[-a_n,a_n] \quad \text{and} \quad \hat{P}_\sigma = \mathbb{BP}(B_{\mathcal{O}_K}^{-1}(P_\sigma)).$$

*Step 4: Compute the integral points $\mathbf{X}^{(1)},\dots,\mathbf{X}^{(M)}$ of $\hat{P}_\sigma$, and for each $1 \leq j \leq M$:*

*(a) Compute the corresponding $\varphi(\sigma) = B_{\mathcal{O}_K}\mathbf{X}_j$ and if*

$$\mathrm{N}(\sigma) > dC\mathrm{N}(\mathbf{y})^{-1/2} \quad \text{or} \quad \varphi(\sigma) \notin P_\sigma,$$

*remove the corresponding $\mathbf{X}^{(j)}$ from the list and repeat for the next $j$, if not, go to the next step.*

*(b) Set $b_{j,i}^{\pm} = \sigma_i x_i \pm y_i a_i$, and let*

$$P_{\rho,j} = [b_{j,1}^-,b_{j,1}^+]\times\cdots\times[b_{j,n}^-,b_{j,n}^+] \quad \text{and} \quad \hat{P}_{\rho,j} = \mathbb{BP}(B_{\mathcal{O}_K}^{-1}(P_{\rho,j})).$$

*(c) Compute the integral points $\mathbf{Y}^{(j,1)},\dots,\mathbf{Y}^{(j,N(j))}$ of $\hat{P}_{\rho,j}$, and for each $1 \leq i \leq N(j)$, compute $\varphi(\rho) = B_{\mathcal{O}_K}\mathbf{Y}^{(j,i)}$ and if $\varphi(\rho) \notin P_{\rho,j}$ remove the corresponding $\mathbf{Y}^{(j,i)}$ from the list.*

*After relabeling the remaining vectors if necessary we find that a closest cusp to $\mathbf{z}$ can now be found corresponding to a pair in the finite set*

$$\left\{(\rho,\sigma) \mid \sigma = B_{\mathcal{O}_K}\mathbf{X}^{(j)}, \rho = B_{\mathcal{O}_K}\mathbf{Y}^{(j,k)},\ 1 \leq j \leq M',\, 1 \leq k \leq N'(j)\right\}$$

*where $M'$ and $N'(j)$ are some positive integers.*

**Remark 11.** Note that we do not make explicit use of the norm bound for $\rho$ here, it is instead part of finding the minimal distance in the final set.

We can now combine Algorithm 10 with the reduction by units and translation described in Section 4 to formulate the complete reduction algorithm.

**Algorithm 12** *(Reduction algorithm). Let $K$ be a fixed totally real number field, let $\mathbf{z} \in \mathbb{H}_K$ and assume all notation is as above,*

*Step 1: Use Algorithm 10 to find the closest cusp to $\mathbf{z}$, say $\mu$.*

*Step 2: Find the cusp representative, $\lambda_j$, corresponding to $\mu$ and $U_\mu \in \Gamma_K$ such that $U_\mu(\mu) = \lambda_j$.*

*Step 3: Set $\mathbf{z}_{\lambda_j} = A_j^{-1}U_\mu\mathbf{z} = \mathbf{x}_{\lambda_j} + i\mathbf{y}_{\lambda_j}$.*

*Step 4: Let $\mathbf{Y} = \mathbf{Y}_\Lambda(\mathbf{y}_{\lambda_j})$ and define $\varepsilon = \varepsilon_1^{b_1}\dots\varepsilon_{n-1}^{b_{n-1}}$ where $b_k = -\left\lfloor\frac{Y_k}{2}\right\rfloor$.*

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

ARTICLE IN PRESS



**Table 1**
Times to find closest cusp of $\mathbf{z} = i\mathbf{1}$ for different fields.

| Field | $\mathbb{Q}(\sqrt{5})$ | $\mathbb{Q}(\sqrt{10})$ | $\mathbb{Q}(\alpha_1)$ | $\mathbb{Q}(\alpha_2)$ |
|---|---|---|---|---|
| Time / ms | 13 ms | 19 ms | 124 ms | 387 s |

*Step 5:* *Set* $\mathbf{z}' = E(\varepsilon)\mathbf{z}_{\lambda_j} = \mathbf{x}' + i\mathbf{y}'$.
*Step 6:* *Let* $\mathbf{X} = \mathbf{X}_{\mathfrak{a}_j^{-2}}(\mathbf{x}')$ *and define* $\alpha = a_1\beta_1 + \cdots + a_n\beta_n$ *where* $a_k = -\lfloor X_k \rfloor$ *and* $\beta_1, \ldots, \beta_n$ *is an integral basis for* $\mathfrak{a}_j^{-2}$.
Step 7: *Set* $A = A_j T^\alpha E(\varepsilon) A_j^{-1} U_\mu$.

Then $A \in \Gamma_K$ and $A\mathbf{z} \in \mathcal{F}_j \subseteq \mathcal{F}$.

### 6.1. A brief analysis of runtime and performance

It is clear that reduction within the cuspidal domain is essentially of constant time with respect to $\mathbf{z}$. The run-time is therefore essentially proportional to the total number of potential $\sigma$s and $\rho$s that are investigated in Algorithm 10 and each of these numbers are proportional to the volumes of the corresponding polytopes. It is of little practical use to make a very precise run-time analysis here but by using appropriate upper bounds it is easy to see that for a fixed totally real number field $K$ the run-time is polynomial in $\|\mathbf{x}\|_\infty, \|\mathbf{y}\|_\infty$ and $\|\mathbf{y}^{-1}\|_\infty$ as $\mathbf{z}$ varies. Similarly, if $\mathbf{z}$ is fixed and we let $K$ vary then the run-time is exponential in the degree of $K$ and $\|B_\Lambda\|_\infty$, and polynomial in $C$, $\left\|B_{\mathcal{O}_K}^{-1}\right\|_\infty$ and $\|B_{\mathcal{O}_K}\|_\infty$. While algebraic quantities like the discriminant and regulator of $K$ do play a direct role also in the reduction by units and translations, these can be bounded by the respective matrix norms.

While a more precise analysis for the dependency on $\mathbf{z}$ is not too difficult to perform, a detailed analysis on the precise dependency on the number field is more complex due to the number of different parameters involved. For testing the runtime in practice it is convenient to consider the point $\mathbf{z} = i\mathbf{1}$ since it will always be closest to both 0 and $\infty$ and the preliminary search using LLL does not provide any better bound. Table 1 contains times to find the closest cusp of $i\mathbf{1}$ for the different fields we consider in Section 7. Here $\alpha_1$ and $\alpha_2$ have minimal polynomials $\alpha_1^3 - \alpha_1^2 - 2\alpha_1 + 1$ and $\alpha_2^3 - 36\alpha_2 - 1$, respectively. For a more systematic comparison regarding the dependency on the discriminant we also compared quadratic fields of class number one and discriminant up to 100. See Table 2. The difference in timing between discriminant 93 and 97 of a factor over 200 is striking. It highlights that the influence of the discriminant is vastly overshadowed by that of the size of the embeddings of the fundamental units. The lengths in question here are $\approx 3.37$ and $\approx 9.32$, respectively, and $\exp(9.3 - 3.3) \approx 403$.

All computations below were performed on a single 2 GHz Xeon E5-2660 core and the reported time is an average of 100 runs.

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

**Table 2**
Times to find closest cusp of $\mathbf{z} = i\mathbf{1}$ for quadratic fields of discriminant $D$ and class number 1.

| D | 5 | 8 | 12 | 13 | 17 | 21 | 24 | 28 | 29 | 33 | 37 | 41 | 44 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Time / ms | 12 | 14 | 14 | 13 | 17 | 14 | 18 | 20 | 14 | 37 | 17 | 47 | 23 |
| D | 53 | 56 | 57 | 61 | 69 | 73 | 76 | 77 | 88 | 89 | 92 | 93 | 97 |
| Time / ms | 15 | 26 | 167 | 30 | 23 | 1087 | 178 | 16 | 201 | 488 | 33 | 24 | 4740 |

### *6.2. A note on the implementation*

The algorithms described above are currently implemented as part of a package in Python with parts written in Cython and are dependent on SageMath [22]. The package is available from [20] and open sourced under GPLv3+.

## 7. Examples

The aim of the examples presented here is to demonstrate how the algorithm works as well as making it easy for readers to verify the correctness. We will consider three examples in detail: first the standard example of $K_1 = \mathbb{Q}(\sqrt{5})$, which has degree 2, discriminant 5 and class number 1, then $K_2 = \mathbb{Q}(\sqrt{10})$ which has degree 2, discriminant 40 and class number 2, followed by $K_3 = \mathbb{Q}(\alpha)$ where $\alpha$ has minimal polynomial $\alpha^3 - \alpha^2 - 2\alpha + 1$, which has degree 3, discriminant 49 and class number 1. The computations involved in these three examples are demonstrated in the accompanying Jupyter notebooks that can be found in [20]

**Example 13.** Consider $K = \mathbb{Q}\left(\sqrt{5}\right)$ with fundamental unit $\varepsilon = \frac{1}{2}(1+\sqrt{5})$, ring of integers $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\varepsilon$ and class number 1. Here

$$B_\Lambda = \begin{pmatrix} \log(\frac{1}{2}(1+\sqrt{5})) & \log(\frac{1}{2}(\sqrt{5}-1)) \end{pmatrix},$$

$$B_{\mathcal{O}_K} = \begin{pmatrix} 1 & \frac{1}{2}\left(1+\sqrt{5}\right) \\ 1 & \frac{1}{2}\left(1-\sqrt{5}\right) \end{pmatrix}, \; B_{\mathcal{O}_K}^{-1} = \frac{1}{-\sqrt{5}} \begin{pmatrix} \frac{1}{2}(1-\sqrt{5}) & -\frac{1}{2}(1+\sqrt{5}) \\ -1 & 1 \end{pmatrix}$$

and it is immediate to see that

$$r_1(B_\Lambda) = r_2(B_\Lambda) \approx 0.48, \quad D_1 = D_2 \approx 1.27, \quad \|B_{\mathcal{O}_K}\|_\infty \approx 2.62, \quad \text{and} \quad \left\|B_{\mathcal{O}_K}^{-1}\right\|_\infty = 1.$$

Consider now Algorithm 10 applied to $\mathbf{z} = \mathbf{y} = i\mathbf{1} \in \mathbb{H}^n$. Since $y_1 = y_2 = 1$ the first bounds are given by $a_1 = a_2 = D_1$ and it can be computed that $P_\sigma$ is the polygon bounded by the vertices

$$B_{\mathcal{O}_K}^{-1}((\pm D_0, \pm D_0)) = \{(0.57, 1.14), (1.27, 0.0), (-0.57, -1.14), (-1.27, 0.0)\}.$$

For this $\mathbf{z}$ the preliminary reduction does not produce any better cusp than $\infty$ and the norm bound is given by $C\mathrm{N}\left(\mathbf{y}\right)^{-1/2} = 1$. The domain $P_\sigma$ and its pre-image together

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

ARTICLE IN PRESS



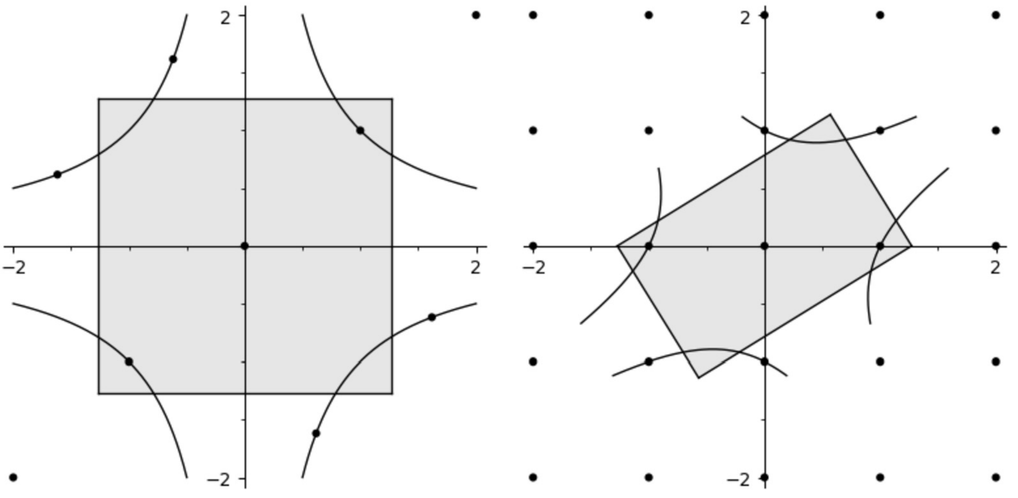


**Fig. 7.1.** $B_{\mathcal{O}_K}(P_\sigma)$ and $P_\sigma$ together with $\mathrm{N}(\sigma) = 1$ for $\mathbf{z} = i\mathbf{1}$ and $K = \mathbb{Q}(\sqrt{5})$.

with the embedded points of $\mathcal{O}_K$ and $\mathbb{Z}^2$ and the curves indicating the norm bound are shown in Fig. 7.1. Note that we show the actual domain $B_{\mathcal{O}_K}^{-1}(P_\sigma)$ and not the bounding box for extra clarity.

It is clear from the figure that the only integral points in $P_\sigma$ are $\mathbf{X}^{(1)} = (0, 0)$, $\mathbf{X}^{(2)} = (1, 0)$ and $\mathbf{X}^{(3)} = (-1, 0)$ so the three candidates for $\sigma$ are 0, 1 and $-1$. The value $\sigma = 0$ of course corresponds to the cusp at infinity so we can choose $\rho = 1$ in this case. For $\sigma = \pm 1$ we get $P_{\rho,2} = P_\sigma$ so the candidates for $\rho$ are 0 and $\pm 1$. The potential cusps are therefore $\infty = (1 : 0)$, $c_1 = (0 : 1)$, $c_2 = (1 : 1)$ and $c_3 = (-1 : 1)$. The corresponding distances are $\Delta(\mathbf{z}, \infty) = \mathrm{N}(\mathbf{y})^{-1/2} = 1$, $\Delta(\mathbf{z}, (0 : 1)) = \mathrm{N}\left(\mathbf{y}\right)^{1/2} = 1$ and

$$\Delta(\mathbf{z}, (1 : 1)) = \mathrm{N}\left(\mathbf{y}^{-1} + \mathbf{y}\right)^{1/2} = 2.$$

Therefore both $\infty = (1 : 0)$ and $0 = (0 : 1)$ are closest cups.

If we consider instead $\mathbf{z} = \frac{1}{2} i\mathbf{1}$ then a preliminary search (using e.g. the LLL method) finds the cusp $0 = (0 : 1)$ and it is easy to see that $\Delta(\mathbf{z}, \infty) = 2$ and $\Delta(\mathbf{z}, 0) = 1/2$. We can therefore apply the algorithm with an initial estimate of $d = 1/2$. This leads to the same bounds for $\sigma$: $|\sigma_i| \leq D_0$ but the bounds for $\rho$ get scaled: $|\rho_i| \leq D_0/2 \approx 0.636$. The candidate cusps are therefore simply $(1 : 0) = \infty$ and $(0 : 1)$ with the closest cusp being $(0 : 1)$.

If we had not performed the initial search and instead simply used $d = \Delta\left(\mathbf{z}, \infty\right) = 2$ for the initial bound we would have obtained 9 candidates for sigma and in the end 9 candidates for closest cusp.

**Example 14.** Consider $K_2 = \mathbb{Q}\left(\sqrt{10}\right)$ with fundamental unit $\varepsilon = 3 + \sqrt{10}$, ring of integers $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{10}$ and class number 2. The cusp representatives are

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

$$\lambda_1 = \infty \quad \text{and} \quad \lambda_2 = (2 : \sqrt{10})$$

Note that the norm of the ideal associated with $\lambda_2$ is $\mathrm{N}\left((2, \sqrt{10})\right) = 2$. We now find that

$$B_\Lambda = \begin{pmatrix} \log((3+\sqrt{10})) & \log(\sqrt{10}-3)) \end{pmatrix},$$

$$B_{\mathcal{O}_K} = \begin{pmatrix} 1 & \sqrt{10} \\ 1 & -\sqrt{10} \end{pmatrix} \quad \text{and} \quad B_{\mathcal{O}_K}^{-1} = \frac{1}{-2\sqrt{10}} \begin{pmatrix} -\sqrt{10} & -\sqrt{10} \\ -1 & 1 \end{pmatrix},$$

and it is immediate to see that

$$r_1(B_\Lambda) = r_2(B_\Lambda) \approx 1.81, \quad D_1 = D_2 \approx 3.51, \quad \|B_{\mathcal{O}_K}\|_\infty \approx 4.16, \quad \text{and} \quad \left\|B_{\mathcal{O}_K}^{-1}\right\|_\infty = 1.$$

Consider now again Algorithm 10 applied to $\mathbf{z} = \mathbf{y} = i\mathbf{1} \in \mathbb{H}^n$. Since $y_1 = y_2 = 1$ the first bounds are given by $a_1 = a_2 = D_0 \approx 3.51$ and $P_\sigma$ is the polygon bounded by the vertices

$$B_{\mathcal{O}_K}^{-1}((\pm D_0, \pm D_0)) \approx \{(-3.51, 0), (0, 1.11), (0, -1.11), (3.51, 0)\}.$$

For this particular $\mathbf{z}$ the preliminary reduction does not produce any better cusp than $\infty$ and the norm bound is given by $C\mathrm{N}(\mathbf{y})^{-1/2} = 2$. The domain $P_\sigma$ and its pre-image together with the embedded points of $\mathcal{O}_K$ and $\mathbb{Z}^2$ are shown in Fig. 7.2. We see that there are only 3 possibilities for $\sigma$: $-1$, 0 and 1 and these result in 10 candidate cusps. Comparing all these we see that the cusps $\infty$ and 0 are both closest with distance $\Delta(\mathbf{z}, \infty) = \Delta(\mathbf{z}, 0) = 1$.

Changing to the point $\mathbf{z} = i\mathbf{\frac{1}{2}}$, the preliminary search finds a tentative closest cusp 0 with a distance of 1/2 so we can use the algorithm with $d = 1/2$, which results in the same bounds for $\sigma$ as before and we find three candidate cusps 0, 1 and $-1$ with the cusp 0 being the unique closest cusp, with distance $\Delta(\mathbf{z}, 0) = 1/2$.

To demonstrate the algorithm works for other cusps than infinity, consider the point $\mathbf{z} = (2.58 + 0.5i, 0.5 + 0.5i)$. The preliminary search gives only the potential closest cusp $\infty$ so we will apply the algorithm with $d = 2$ and the norm bound $|\sigma_1\sigma_2| \le 8$. We find 13 candidates for $\sigma$ and 35 distinct candidate cusps, from which we find that $\mu = (\sqrt{10} : \sqrt{10} + 2)$ is the closest, with distance $\approx 1.59$. It is not hard to check that $\mu$ is equivalent to $\lambda_2$ under the element

$$\begin{pmatrix} -5 & -2\sqrt{10}+9 \\ -2\sqrt{10}+1 & 4\sqrt{10}-10 \end{pmatrix} \in \Gamma_K.$$

Applying the complete reduction map to $\mathbf{z}$ gives $\mathbf{w} = B\mathbf{z}$ with $\mathbf{w} \approx (-0.669 + 0.036i, 0.709 + 0.004i)$ and

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

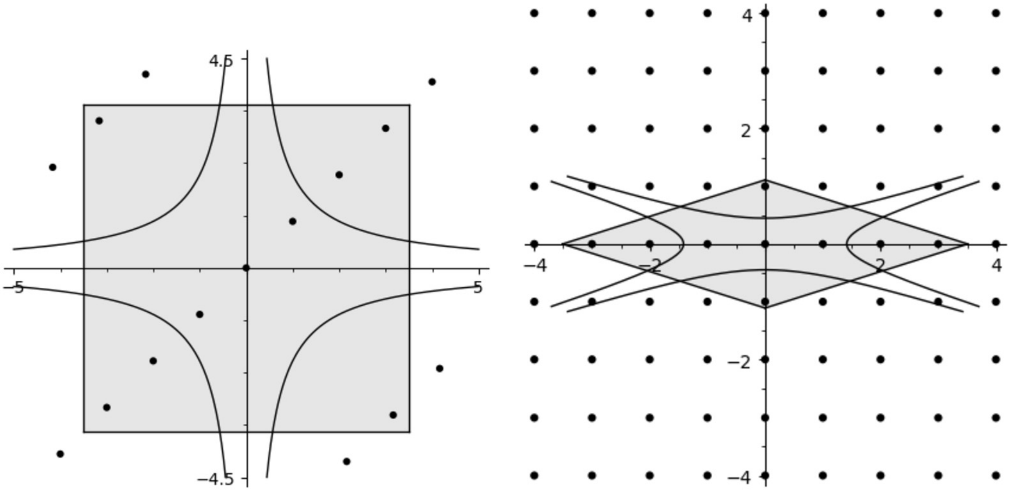


**Fig. 7.2.** $B_{\mathcal{O}_{K_2}^{-1}}(P_\sigma)$ and $P_\sigma$ together with the curve $\mathrm{N}(\sigma) = 2$ for $\mathbf{z} = i\mathbf{1}$, $K_2 = \mathbb{Q}(\sqrt{10})$.

$$B = \begin{pmatrix} -2\sqrt{10} - 9 & 9 \\ -4\sqrt{10} - 9 & 4\sqrt{10} \end{pmatrix} \in \Gamma_K.$$

**Example 15.** To demonstrate that the method works also in degree 3, consider $K_3 = \mathbb{Q}(\alpha)$ where $\alpha$ has minimal polynomial $\alpha^3 - \alpha^2 - 2\alpha + 1$. This field has degree 3, class number 1, discriminant 49, fundamental units $\varepsilon_1 = 2 - \alpha^2$ and $\varepsilon_2 = \alpha^2 - 1$ and $\mathcal{O}_K$ has an integral basis

$$\beta_1 = 1,\ \beta_2 = \alpha,\ \beta_3 = \alpha^2 - 2.$$

The real embeddings of $\alpha$ are approximately $(-1.247, 0.445, 1.802)$ and we find the relevant numerical bounds to be:

$$\mathbf{r}(B_\Lambda) \approx (1.40, 0.810, 1.03), \quad \mathbf{D} \approx (2.01, 1.499, 1.674),$$
$$\|B_{\mathcal{O}_K}\|_\infty \approx 4.05, \text{ and } \left\|B_{\mathcal{O}_K}^{-1}\right\|_\infty = 1.$$

Let $\mathbf{z} = i\mathbf{1}$ and apply Algorithm 10 to find closest cusps. In the first step we find 5 candidates for $\sigma$. See Fig. 7.3, which shows the polyhedron together with the surfaces $\mathrm{N}(\sigma) = 1$. The two points which do not satisfy the norm bound are drawn in lighter gray, the others in black. In the end we find 8 candidates for the closest cusp and we find (as usual) that the cusps $\infty$ and 0 are both closest with a distance of 1.

**Example 16.** Just to give an idea of how it works in a more complicated example, consider $K = \mathbb{Q}(\alpha)$ where $\alpha$ has a minimal polynomial $x^3 - 36x - 1$. Then $K$ has discriminant 20733, class number 5 and its label in the LMFDB is 3.3.20733.1. The fundamental units are $\varepsilon_1 = -\alpha$ and $\varepsilon_2 = -\alpha - 6$ and $\mathcal{O}_K$ has an integral basis

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

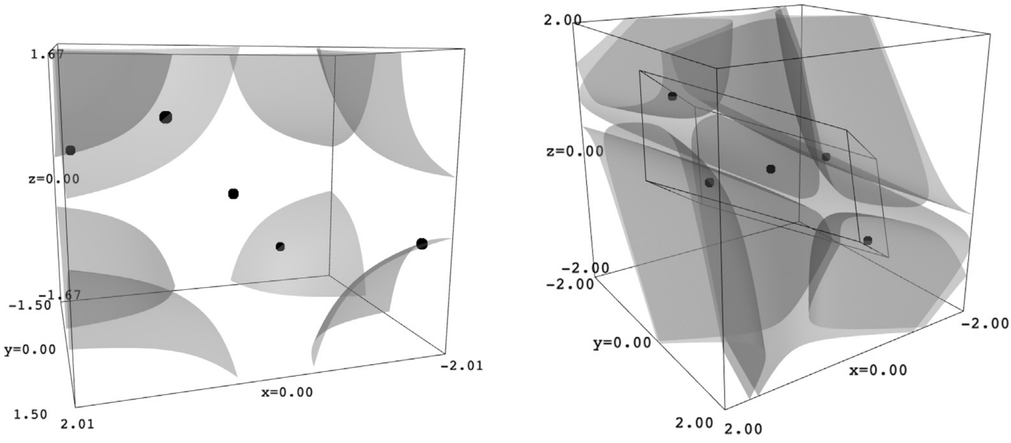


**Fig. 7.3.** $B_{\mathcal{O}_{K_3}}(P_\sigma)$ and $P_\sigma$ for $\mathbf{z} = i\mathbf{1}$, $K_3 = \mathbb{Q}(\alpha)$ with $\alpha^3 - \alpha^2 - 2\alpha + 1$.

$$\beta_1 = 1, \ \beta_2 = \alpha, \ \beta_3 = \frac{1}{3}\left(\alpha^2 + \alpha - 23\right).$$

The real embeddings of $\alpha$ are approximately $(-5.986, -0.028, 6.014)$ and we find the relevant numerical bounds to be:

$$\|B_\Lambda\|_\infty \approx 6.06, \quad D_0 \approx 52.22, \quad \|B_{\mathcal{O}_K}\|_\infty \approx 13.41, \quad \text{and} \quad \left\|B_{\mathcal{O}_K}^{-1}\right\|_\infty = 1.$$

Using Algorithm 10 with $\mathbf{z} = i\mathbf{1}$ we find 9 candidates for $\sigma$, in total 3396 candidate cusps and as usual the cusps 0 and $\infty$ are both closest with distance 1.

## References

[1] O. Blumenthal, Über Modulfunktionen von mehreren Veränderlichen, Math. Ann. 56 (4) (1903) 509–548, https://doi.org/10.1007/BF01444306.

[2] F. Bouyer, M. Streng, Examples of CM curves of genus two defined over the reflex field, LMS J. Comput. Math. 18 (1) (2015) 507–538, https://doi.org/10.1112/S1461157015000121.

[3] H. Cohn, A numerical survey of the floors of various Hilbert fundamental domains, Math. Comput. 19 (1965) 594–605, https://doi.org/10.2307/2003942.

[4] H. Cohn, On the shape of the fundamental domain of the Hilbert modular group, in: Proc. Sympos. Pure Math., vol. VIII, Amer. Math. Soc., Providence, R.I., 1965, pp. 190–202.

[5] J.E. Cremona, M.T. Aranés, Congruence subgroups, cusps and Manin symbols over number fields, in: Computations with modular forms, in: Contrib. Math. Comput. Sci., vol. 6, Springer, Cham, 2014, pp. 109–127.

[6] J.I. Deutsch, A computational approach to Hilbert modular group fixed points, Math. Comput. 71 (239) (2002) 1271–1280, https://doi.org/10.1090/S0025-5718-01-01403-X.

[7] J.I. Deutsch, Conjectures on the fundamental domain of the Hilbert modular group, Comput. Math. Appl. 59 (2) (2010) 700–705, https://doi.org/10.1016/j.camwa.2009.10.023.

[8] E. Freitag, Hilbert Modular Forms, Springer-Verlag, Berlin, 1990.

[9] F. Götzky, Über eine zahlentheoretische Anwendung von Modulfunktionen zweier Veränderlicher, Math. Ann. 100 (1) (1928) 411–437.

[10] X. Guitart, M. Masdeu, Elementary matrix decomposition and the computation of Darmon points with higher conductor, Math. Comput. 84 (292) (2015) 875–893, https://doi.org/10.1090/S0025-5718-2014-02853-6.

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011

ARTICLE IN PRESS



[11] D.A. Hejhal, On the calculation of Maass cusp forms, in: Hyperbolic Geometry and Applications in Quantum Chaos and Cosmology, in: London Math. Soc. Lecture Note Ser., vol. 397, Cambridge Univ. Press, Cambridge, 2012, pp. 175–185.

[12] O. Herrmann, Eine metrische Charakterisierung eines Fundamentalbereichs der Hilbertschen Modulgruppen, Math. Z. 60 (1954) 148–155.

[13] E. Jespers, A. Kiefer, A. del Río, Presentations of groups acting discontinuously on direct products of hyperbolic spaces, Math. Comput. 85 (301) (2016) 2515–2552, https://doi.org/10.1090/mcom/3071.

[14] B. Liehl, On the group $\mathrm{SL}_2$ over orders of arithmetic type, J. Reine Angew. Math. 323 (1981) 153–171, https://doi.org/10.1515/crll.1981.323.153.

[15] H. Maass, Über Gruppen von hyperabelschen Transformationen, Sitzungsber. Heidelb. Akad. Wiss. 1940 (2) (1940) 26.

[16] J. Quinn, A. Verjovsky, Cusp shapes of Hilbert-Blumenthal surfaces, Geom. Dedic. 206 (2020) 27–42, https://doi.org/10.1007/s10711-019-00474-w.

[17] C.L. Siegel, Advanced Analytic Number Theory, 2nd edition, Tata Institute of Fundamental Research Studies in Mathematics, vol. 9, Tata Institute of Fundamental Research, Bombay, 1980.

[18] N.-P. Skoruppa, F. Strömberg, H. Boylan, Dimension formulas for vector valued Hilbert modular forms, in preparation, 2021.

[19] F. Strömberg, Dimension formulas and kernel functions for Hilbert modular forms, in: Automorphic Forms and Related Topics, in: Contemp. Math., vol. 732, Amer. Math. Soc., Providence, RI, 2019, pp. 229–243.

[20] F. Strömberg, Algorithms for Hilbert modular groups, https://github.com/fredstro/hilbertmodgroup, 2021.

[21] T. Tamagawa, On Hilbert's modular group, J. Math. Soc. Jpn. 11 (1959) 241–246.

[22] The Sage Development Team, Sage Mathematics Software (Version 9.4), http://www.sagemath.org, 2021.

[23] G. van der Geer, Hilbert Modular Surfaces, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) (Results in Mathematics and Related Areas (3)), vol. 16, Springer-Verlag, Berlin, 1988.

[24] L.N. Vaseršteĭn, The group $SL_2$ over Dedekind rings of arithmetic type, Mat. Sb. (N.S.) 89 (131) (1972) 313–322, 351.

Please cite this article in press as: F. Strömberg, A reduction algorithm for Hilbert modular groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.02.011