Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

On the computation of Hermite-Humbert constants for real quadratic number fields

par Marcus WAGNER et Michael E. POHST

Abstract. We present algorithms for the computation of extreme binary Humbert forms in real quadratic number fields. With these algorithms we are able to compute extreme Humbert forms for the number fields $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(\sqrt{17})$. Finally we compute the Hermite-Humbert constant for the number field $\mathbb{Q}(\sqrt{13})$.

1. Introduction

A new invariant of number fields, called Hermite-Humbert constant, was introduced by P. Humbert in 1940. This constant is an analogue to the Hermite constant for $\mathbb{Q}$. In [H] Humbert describes a generalization of the reduction theory for quadratic forms over $\mathbb{Z}$ where he considers totally positive forms, called Humbert forms, with integral entries in a given number field K. He deduces an analogous reduction theory and the existence of the Hermite-Humbert constant.
In this work we compute extreme binary Humbert forms for the number fields $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(\sqrt{17})$ and the Hermite-Humbert constant $\gamma_{K,2}$ for $K = \mathbb{Q}(\sqrt{13})$. In [BCIO] it is shown that finding Hermite-Humbert constants of real quadratic number fields is tantamount to looking for extreme Humbert forms. Their existence is proved in [Ica]. Following the precedence of Voronoï a characterization of extreme Humbert forms is given in [C] by introducing two properties of extreme Humbert forms, namely perfection and eutacticity. With these properties we are able to make a unique characterization of extreme Humbert forms: a Humbert form is extreme if and only if it is both, perfect and eutactic.

2. The theoretical background

Let $\mathcal{P}$ denote the set of positive real binary Humbert forms, i.e. $S = (S_1, S_2) \in \mathcal{P}$ with positive definite 2×2 real matrices S_1 and S_2. If K denotes a real quadratic number field and $\mathcal{O}_K$ its maximal order, we denote with $S[x]$ the product $x^t S_1 x \cdot x'^t S_2 x'$ for any $x \in \mathcal{O}_K^2$, where x' denotes the conjugate vector of x and we let $\det S$ be the product of the determinants

$\det S_1$ and $\det S_2$. In the same way U' denotes a matrix with conjugated entries of a matrix $U \in K^{2\times 2}$. Let

$$m(S) := \min\{S[x] : \ 0 \neq x \in \mathcal{O}_K^2\}$$

denote the minimum of a given Humbert form S, then

$$M(S) := \{[x] \in \mathcal{O}_K^2 \mid S[x] = m(S)\}$$

denotes a set of equivalence classes

$$[x] := \{y \in \mathcal{O}_K^2 \mid y = \epsilon x, \ \epsilon \in \mathcal{O}_K^\times\}$$

where the elements of $M(S)$, respectively their representatives, are called minimal vectors of S. To avoid superfluous notation we denote the elements $[x]$ of $M(S)$ only with x. If a tuple $U := (U_1, U_2) \in \mathrm{GL}(2, \mathcal{O}_K)^2$ is given we can make unimodular transformations from a Humbert form S to another denoted by

$$S[U] := (S[U_1], S[U_2]) := (U_1^t S_1 U_1, U_2^t S_2 U_2^t).$$

By scaling we mean multiplication of a given Humbert form $S = (S_1, S_2)$ with an element $\lambda = (\lambda_1, \lambda_2) \in (\mathbb{R}^{>0})^2$ to obtain another Humbert form

$$\lambda S := (\lambda_1 S_1, \lambda_2 S_2).$$

We note that for a given Humbert form S the set $M(S)$ is finite which is shown in [Ica]. The following theorem is due to Humbert. He proved the existence of Hermite-Humbert constants:

Theorem 1. *For any $S \in \mathcal{P}$ and any real quadratic number field K of discriminant d_K there is a constant $C \in \mathbb{R}^{>0}$ with $C < 2^{10}|d_K|^2$ such that*

$$S[x] \leq C\sqrt{\det S} \quad \forall x \in M(S). \tag{1}$$

There are better upper bounds for C, see [Co2] and [Ica]. We use the estimate $C \leq \frac{1}{2}|d_K|$ from [Co2]. With theorem 1 we are able to define a map from $\mathcal{P}$ to $\mathbb{R}^{>0}$ in the following way.

Definition & Proposition 2. *Let $S \in \mathcal{P}$ and*

$$\gamma_{_K} : \mathcal{P} \longrightarrow \mathbb{R}^{>0}, \quad \gamma_{_K}(S) = \frac{m(S)}{\sqrt{\det S}},$$

then $\gamma_{_K}$ is invariant under unimodular transformations and scaling.

Now we are able to define the Hermite-Humbert constant as

$$\gamma_{K,2} = \sup_{S\in\mathcal{P}} \gamma_{_K}(S). \tag{2}$$

Any Humbert form S for which equality holds in (2) is called critical. The existence of such forms is shown in [Ica]. The value $\gamma_{_K}(S)$ of a critical Humbert form S is a global maximum of $\gamma_{_K}$. Forms for which $\gamma_{_K}$ achieves

a local maximum are called extreme. For characterizing extreme forms we introduce two properties: perfection and eutacticity. If $S = (S_1, S_2) \in \mathcal{P}$ and $x \in M(S)$, then

$$\left(\frac{xx^t}{S_1[x]}, \frac{x'x'^t}{S_2[x']} \right)$$

is a semi-positive definite Humbert form. The set of such forms of a given $S \in \mathcal{P}$ will be denoted with X_S. Now perfection means

$$\dim \sum_{X \in X_S} \mathbb{R}X = 5$$

and eutacticity means that there is a representation

$$S^{-1} = (S_1^{-1}, S_2^{-1}) = \sum_{X \in X_S} \rho_X X$$

with $\rho_X \in \mathbb{R}^{>0}$ for all $X \in X_S$.

Definition 3. *If* $(S_1, S_2) \in (\mathbb{R}^{2\times 2})^2$ *with*

$$S_i = \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix} \quad (i = 1, 2)$$

then we define the map

$$\Phi : \ (\mathbb{R}^{2\times 2})^2 \longrightarrow \mathbb{R}^6, \quad (S_1, S_2) \longmapsto (a_1, b_1, c_1, a_2, b_2, c_2)^t.$$

Now perfection and eutacticity become

$$\dim \sum_{X \in X_S} \mathbb{R}\Phi(X) = 5 \quad \text{and} \quad \Phi(S^{-1}) = \sum_{X \in X_S} \rho_X \Phi(X).$$

This means a Humbert form S is eutactic if $\Phi(S^{-1})$ is in the interior of the linear convex hull of the points $\Phi(X)$ where $X \in X_S$. The following theorem of [C] characterizes extreme forms:

Theorem 4. *A Humbert form is extreme if and only if it is both, eutactic and perfect. An extreme Humbert form of a real quadratic number field has at least 5 minimal vectors.*

Now we need the definition of being equivalent for two Humbert forms S und T:

Definition 5. *Two Humbert forms* S *and* T *are called* ***equivalent****, if there is a tupel* $U := (U_1, U_2) \in \mathrm{GL}(2, \mathcal{O}_K)^2$ *with* $U_2 = U_1'$ *and*

$$T = S[U]$$

or there is $\lambda = (\lambda_1, \lambda_2) \in (\mathbb{R}^{>0})^2$ *such that* $S = \lambda T$.

In [C] is shown that there is only a finite number of extreme forms up to equivalence. This suggests to look for a suitable set of representatives of extreme Humbert forms. With the next lemmata we are able to determine such a set and a finite set M which contains all minimal vectors for each element of it. Before we start we need one more definition:

Definition 6. *Two elements $x, y \in \mathcal{O}_K^2$ are called* ***a unimodular pair*** *if they are a $\mathcal{O}_K$-basis of $\mathcal{O}_K^2$, i.e. $\mathcal{O}_K^2 = \mathcal{O}_K x \oplus \mathcal{O}_K y$.*

With $\epsilon_0 > 1$ we denote the fundamental unit of the real quadratic number field K. The following lemma is proved in [BCIO]:

Lemma 7. *Let $h_K = 1$. If any extreme Humbert form has a unimodular pair of minimal vectors then it is equivalent to a form*

$$S = \left(\begin{pmatrix} 1 & b_1 \\ b_1 & c \end{pmatrix}, \begin{pmatrix} 1 & b_2 \\ b_2 & c^{-1} \end{pmatrix} \right) \tag{3}$$

with $\epsilon_0^{-1} \leq c < \epsilon_0$. The standard basis vectors e_1 and e_2 are contained in the set $M(S)$ and for any other minimal vector $x = (x_1, x_2)^t \in \mathcal{O}_k^2$ we have

$$|\mathrm{N}_{K/\mathbb{Q}}(x_1)| \leq \gamma_{K,2}, \quad |\mathrm{N}_{K/\mathbb{Q}}(x_2)| \leq \gamma_{K,2}$$

and

$$|x_2^{(1)}| < \frac{\sqrt{\epsilon_0}\gamma_{K,2}}{|x_1^{(2)}|}, \quad |x_2^{(2)}| < \frac{\sqrt{\epsilon_0}\gamma_{K,2}}{|x_1^{(1)}|}.$$

We denote the obtained set of such representatives with $\mathfrak{S}$. For a restriction of the finite set M of minimal vectors for each element of $\mathfrak{S}$ we can make use of the following lemma (see [BCIO]):

Lemma 8. (1) *Let $S = (S_1, S_2) \in \mathcal{P}$ with*

$$S_i = \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix}$$

for $i = 1, 2$ and $u = (u_1, u_2)^t \in \mathcal{O}_K^2$. Then

$$\begin{aligned} |\mathrm{N}_{K/\mathbb{Q}}(u_1)| &\leq \sqrt{\tfrac{c_1 c_2 S[u]}{m(S)^2}}\gamma_{K,2}, \\ |\mathrm{N}_{K/\mathbb{Q}}(u_2)| &\leq \sqrt{\tfrac{a_1 a_2 S[u]}{m(S)^2}}\gamma_{K,2}, \\ |u_1^{(1)} u_2^{(2)}| &\leq \sqrt{\tfrac{a_2 c_1 S[u]}{m(S)^2}}\gamma_{K,2}, \\ |u_1^{(2)} u_2^{(1)}| &\leq \sqrt{\tfrac{a_1 c_2 S[u]}{m(S)^2}}\gamma_{K,2}. \end{aligned}$$

(2) *Let $u = (u_1, u_2)^t$, $v = (v_1, v_2)^t \in \mathcal{O}_K^2$ be minimal vectors of S with $v \notin \mathcal{O}_K^\times u$ and*

$$U = \begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \end{pmatrix},$$

then

$$|\mathrm{N}_{K/\mathbb{Q}}(\det U)| \leq \gamma_{K,2}.$$

By Theorem 4 we know every extreme Humbert form has at least 5 minimal vectors. Now we are able to compute all possible extreme forms as follows if we assume every Humbert form has a unimodular pair of minimal vectors:

(1) determine the finite set M of all possible minimal vectors for each element of $\mathfrak{S}$
(2) for any 3-set $T = \{u_1, u_2, u_3\} \subseteq M \backslash \{e_1, e_2\}$ we have to solve polynomial equations $S[u_i] = 1$ in the unknowns of $S \in \mathfrak{S}$ where

$$S = \left(\begin{pmatrix} 1 & b_1 \\ b_1 & c \end{pmatrix}, \begin{pmatrix} 1 & b_2 \\ b_2 & c^{-1} \end{pmatrix} \right)$$

and $i = 1, 2, 3$
(3) finally we have to test whether the obtained Humbert forms are eutactic and perfect.

A last step should be done: if we have two perfect Humbert forms S and T we need an algorithm which decides whether T and S are equivalent. We consider two 3-sets $W = \{w_1, w_2, w_3\} \subseteq M(T)$ and $V = \{v_1, v_2, v_3\} \subseteq M(S)$ of minimal vectors. If S and T are unimodular equivalent then there is a matrix $U \in \mathrm{GL}(2, \mathcal{O}_K)$ with

$$U w_i = \epsilon_i v_i \tag{4}$$

for $i = 1, 2, 3$ and suitable units $\epsilon_i \in \mathcal{O}_K^\times$. Now two perfect Humbert forms S and T are equivalent if and only if there exists a matrix $U \in \mathrm{GL}(2, \mathcal{O}_K)$ with $U \cdot M(T) = M(S)$.

3. The algorithms

In this section K always denotes a real quadratic number field with $h_K = 1$ and $\epsilon_0 > 1$ the fundamental unit of the maximal order $\mathcal{O}_K$.

Next we want to develop an algorithm for computing extreme Humbert forms. The main algorithm splits in several subalgorithms. The first subalgorithm for computing the set M and all 3-sets is algorithm 10. After computing all 3-sets of M we have to compute real solutions of the polynomial equations obtained by all triples of M to construct Humbert forms. Finally we compute minimal vectors with algorithm 14 and if necessary eutactic coefficients.

Algorithm 9 (Main Algorithm)**.**
Input: The maximal order $\mathcal{O}_K$ of a real quadratic number field K
Output: A set of all eutactic and perfect Humbert forms of K up to equivalence having a unimodular pair of minimal vectors

- $T \leftarrow$ All 3-sets of M
- $H_1 \leftarrow$ set of Humbert forms obtained by the real solutions of the polynomial equations
- $H_2 \leftarrow \{S = (S_1, S_2) \in H_1 \mid m(S) = 1\}$
- $H_3 \leftarrow \big\{(h_1, h_2) \mid h_2 \in H_2,\ h_1 = \text{minimal vectors of } h_2 \text{ and } |h_1| > 4\big\}$
- $H_4 \leftarrow \{h = (h_1, h_2) \in H_3 \mid h_2 \text{ is perfect and eutactic }\}$
- $H_5 \leftarrow$ set of non-equivalent Humbert forms
- Return H_4

3.1. Computing of all 3-sets of M. In this section we describe the algorithm to compute all suitable 3-sets of M. We make use of the results of lemma 7 and lemma 8. Note that we assume every Humbert form has got a unimodular pair of minimal vectors.

Algorithm 10 (3-sets of M)**.**
Input: An integral basis $1, \omega$ of the maximal order $\mathcal{O}_K$ of a real quadratic number field K, the fundamental unit ϵ_0

Output: All suitable 3-sets of M

- $M \leftarrow \emptyset, \quad X, Y \leftarrow \{[\alpha] \mid \alpha \in \mathcal{O}_K \text{ with } 0 < |\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq \frac{d_K}{2}\}$

- For all $x \in X$ do
  For all $y \in Y$ do
  if $\exists k \in \mathbb{Z}$ with $|\big(y\epsilon_0^k\big)^{(1)}| < \frac{\sqrt{\epsilon_0} d_K}{x^{(2)} 2}$ and $|\big(y\epsilon_0^k\big)^{(2)}| < \frac{\sqrt{\epsilon_0} d_K}{x^{(1)} 2}$ then
  $M \leftarrow M \cup \{(x, y\epsilon_0^k)^t\}$

- $T \leftarrow$ set of all 3-sets of M

- $S \leftarrow \emptyset$

- For all $A = \{\alpha_i \mid \alpha_i \in \mathcal{O}_K^2,\ i = 1, 2, 3\} \in T$ do
  $\Psi \leftarrow \{(\alpha_i, \alpha_j) \in \mathrm{GL}(2, K) \mid i, j \in \{1, 2, 3\}\}$
  If $\Psi = \emptyset$ or for any $X \in \Psi$ there holds $|\mathrm{N}_{K/\mathbb{Q}}(\det X)| > \frac{d_K}{2}$ then
  $S \leftarrow S \cup \{A\}$
  Else

For $X = (\alpha_i, \alpha_j) \in \Psi$ $(i, j \in \{1, 2, 3\}, i \neq j)$ do
  $\alpha \leftarrow A \backslash \{\alpha_i, \alpha_j\}$
  If $\lambda = (\lambda_1, \lambda_2)^t \in K^2$ exists with $\lambda_1 \lambda_2 = 0$ where $\alpha = X\lambda$ then
    $S \leftarrow S \cup \{A\}$

- Return $T \backslash S$

3.2. Unimodular equivalent Humbert forms. Now we describe an algorithm which decides whether two perfect Humbert forms S and T are unimodular equivalent. Let $A = \{a_1, a_2, a_3\} \subseteq M(S)$ and let us assume there holds

$$\lambda_2 a_2 = a_1 \tag{5}$$

with $\lambda_2 \in K$. If $\lambda_2 = \frac{\lambda_{21}}{\lambda_{22}}$ $(\lambda_{22}, \lambda_{21} \in \mathcal{O}_K, \lambda_{22} \neq 0)$ with $\gcd(\lambda_{22}, \lambda_{21}) = 1$ then $a_1 = \lambda_{21}\mu$ for some $\mu \in \mathcal{O}_K^2$. Now we get

$$S[a_1] = \mathrm{N}_{K/\mathbb{Q}}(\lambda_{21})^2 S[\mu]$$

and we obtain $|\mathrm{N}_{K/\mathbb{Q}}(\lambda_{21})| = 1 = |\mathrm{N}_{K/\mathbb{Q}}(\lambda_{22})|$. Together this means

$$\lambda_2 a_2 = a_1 \Rightarrow [a_1] = [a_2]. \tag{6}$$

The same holds if we change the role of the a_i $(i = 1, 2, 3)$. If $A = \{a_1, a_2, a_3\} \subseteq M(S)$ and $B = \{b_1, b_2, b_3\} \subseteq M(T)$ then let us assume without loss of generality the first two element of A and B are K-linear independent. Now we have a representation of the third element of each set with the both first elements. It is easy to see that if a matrix $U \in \mathrm{GL}(2, \mathcal{O}_K)$ exists with respect to (4) then for the matrices $X := (a_1, a_2)$ and $Y := (b_1, b_2)$ there holds $YX^{-1} \in \mathrm{GL}(2, \mathcal{O}_K)$. If we assume a $U \in \mathrm{GL}(2, \mathcal{O}_K)$ with respect to (4) exists we have

$$U(a_1, a_2, a_3) = (\epsilon_1 b_1, \epsilon_2 b_2, b_3) \quad (\epsilon_1, \epsilon_2 \in \mathcal{O}_K^\times)$$

and with $a_3 = X\lambda$ and $b_3 = Y\mu$ we get $\lambda = (\lambda_1, \lambda_2)^t, \mu = (\mu_1, \mu_2)^t \in K^2$ with $\lambda_1, \lambda_2, \mu_1, \mu_2 \neq 0$ because of (6). Now we obtain

$$\epsilon_1 = \frac{\mu_1}{\lambda_1} \text{ and } \epsilon_2 = \frac{\mu_2}{\lambda_2}.$$

Finally we have to test whether ϵ_1 and ϵ_2 are units in $\mathcal{O}_K$ and

$$\left((\epsilon_1 b_1, \epsilon_2 b_2) X^{-1}\right) M(S) = M(T).$$

Algorithm 11 (Equivalence of Humbert Tupels)**.**

Input: The sets $M(S)$ and $M(T)$ of two perfect Humbert forms S and T of a real quadratic number field K

Output: $U \in \mathrm{GL}(2, \mathcal{O}_K)$ with $U \cdot M(S) = M(T)$ if S and T are unimodular equivalent, false otherwise

- $S \leftarrow \emptyset$
- For all $A = \{a_i \mid a_i \in \mathcal{O}_K^2,\ i = 1,2,3\} \subseteq M(S)$
  For all $B = \{b_i \mid b_i \in \mathcal{O}_K^2,\ i = 1,2,3\} \subseteq M(T)$ do
  $\Psi_1 \leftarrow \{(a_i, a_j) \in \mathrm{GL}(2,K) \mid i,j \in \{1,2,3\}\}$
  $\Psi_2 \leftarrow \{(b_i, b_j) \in \mathrm{GL}(2,K) \mid i,j \in \{1,2,3\}\}$
  For $X = (a_i, a_j) \in \Psi_1$ and $Y = (b_k, b_l) \in \Psi_2$ do
  If $|\mathrm{N}_{K/\mathbb{Q}}(\det\ YX^{-1})| = 1$ then
  $a \leftarrow A \backslash \{a_i, a_j\}$
  $b \leftarrow B \backslash \{b_k, b_l\}$
  $\lambda \leftarrow (\lambda_1, \lambda_2)^t \in K^2$ with $\lambda_1\lambda_2 \neq 0$ where $a = X\lambda$
  $\mu \leftarrow (\mu_1, \mu_2)^t \in K^2$ with $\mu_1\mu_2 \neq 0$ where $b = Y\mu$
  $\epsilon_1 \leftarrow \frac{\mu_1}{\lambda_1}$,
  $\epsilon_2 \leftarrow \frac{\mu_2}{\lambda_2}$
  If $\epsilon_1, \epsilon_2 \in \mathcal{O}_K^\times$
  If $(\epsilon_1 b_k, \epsilon_2 b_l)X^{-1} \cdot M(S) = M(T)$ then
  Return$((\epsilon_1 b_k, \epsilon_2 b_l)X^{-1})$
- Return false

3.3. Computing minimal vectors. Next we want to compute minimal vectors of a given $S \in \mathcal{P}$. For doing this we need a constructive proof for the finiteness of minimal vectors of a given Humbert form. The reason for this is that we need the quantities which are involved in this proof for the following algorithm which computes minimal vectors.

Lemma 12. *Let $S = (S_1, S_2) \in \mathcal{P}$, $C \in \mathbb{R}^{>0}$ and K be a real quadratic number field. Then the set*

$$\{x \in \mathcal{O}_K^2 \mid S_1[x] + S_2[x'] \leq C\} \tag{7}$$

is finite.

Proof. For all $T \in \mathbb{R}^{2\times 2}$ we denote with $\underline{\|T\|}$ the value

$$\min_{x \neq 0} \frac{\|Tx\|_2}{\|x\|_2} \quad \forall\, x \in \mathbb{R}^2.$$

If T is a regular matrix then we have

$$\underline{\|T\|} = \min_{x \neq 0} \frac{\|Tx\|_2}{\|x\|_2} = \min_{y \neq 0} \frac{\|y\|_2}{\|T^{-1}y\|_2} = \|T^{-1}\|_2^{-1}$$

with $y = Tx$. If we consider the Cholesky decompositions for $S_i = R_i^t R_i$ with $R_i \in \mathrm{GL}(2,\mathbb{R})$ $(i = 1, 2)$, we get

$$S_1[x] = \left\|R_1 x\right\|_2^2 \geq \underline{\left\|R_1\right\|}^2 \left\|x\right\|_2^2 = \left\|R_1^{-1}\right\|_2^{-2} \left\|x\right\|_2^2 \tag{8}$$

and the same holds for $S_2[x']$. For the computation of $\left\|R_i^{-1}\right\|_2$ we need the well known estimate

$$\left\|R_i\right\|_2 \leq \left(\left\|R_i\right\|_\infty \left\|R_i\right\|_1\right)^{\frac{1}{2}} \quad (i = 1, 2)$$

and now we get with (8)

$$S_1[x] \geq \left\|R_1^{-1}\right\|_2^{-2} \left\|x\right\|_2^2 \geq \left(\left\|R_1^{-1}\right\|_\infty \left\|R_1^{-1}\right\|_1\right)^{-1} \left\|x\right\|_2^2$$

where the same holds again for $S_2[x']$. If $m := \min_{i=1,2}\left(\left\|R_i^{-1}\right\|_\infty \left\|R_i^{-1}\right\|_1\right)^{-1}$ we get with $x = (a, b)^t \in \mathcal{O}_K^2$

$$m\Big(a^2 + a'^2 + b^2 + b'^2\Big) = m\Big(\left\|x\right\|_2^2 + \left\|x'\right\|_2^2\Big) \leq S_1[x] + S_2[x'] \leq C \tag{9}$$

and further

$$a^2 + a'^2 = (a, a')(a, a')^t = \underbrace{\left(\begin{pmatrix} 1 & 1 \\ \omega & \omega' \end{pmatrix}\begin{pmatrix} 1 & \omega \\ 1 & \omega' \end{pmatrix}\right)}_{:=A}[(a_1, a_2)^t] \tag{10}$$

with $a = a_1 + a_2\omega$ for an integral basis $\{1, \omega\}$ of $\mathcal{O}_K$ and $a_1, a_2 \in \mathbb{Z}$. We know the matrix A is a positive definite form in $\mathbb{Z}$ because the trace of integral elements of a given maximal order are rational integral elements. With (9) and (10) we obtain for any element $z = (x_1 + x_2\omega, y_2 + y_2\omega)^t$ $(x_1, x_2, y_1, y_2 \in \mathbb{Z})$ of the set in (7) the condition

$$A[(x_1, x_2)^t] \leq \frac{C}{m} \text{ and } A[(y_1, y_2)^t] \leq \frac{C}{m} \tag{11}$$

and the set of solutions of these inequalities is finite and so the set in (7) is finite too. □

The next lemma motivates lemma 12.

Lemma 13. *Let $S = (S_1, S_2) \in \mathcal{P}$. Then there exists a constant $\alpha \in \mathbb{R}^{>0}$ such that suitable representants of the elements of the set $M(S)$ are contained in the set*

$$\left\{x \in \mathcal{O}_K^2 \mid S_1[x] + S_2[x'] \leq \alpha\right\}. \tag{12}$$

With the last two lemmata we are able to compute minimal vectors of a given $S \in \mathcal{P}$.

Algorithm 14 (Minimal Vectors)**.**

Input: A Humbert form $S = (S_1, S_2) \in \mathcal{P}$, the maximal order $\mathcal{O}_K$ with integral basis $\{1, \omega\}$, α and m as in lemma 12 and lemma 13

Output: The set $J \subseteq \mathcal{O}_K^2$ of all minimal vectors of S

- $I, J \leftarrow \emptyset$
  $S_i \leftarrow CS_i \quad (i = 1, 2)$ where $S_i = \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix}$ and $C = (\max\{a_1, a_2\})^{-1}$
  $\epsilon_0 \leftarrow$ the fundamental unit ϵ of $\mathcal{O}_K$ with $\epsilon > 1$
  $m \leftarrow \min_{i=1,2}\left(\left\|R_i^{-1}\right\|_\infty \left\|R_i^{-1}\right\|_1\right)^{-1}$
  where $S_i = R_i^t R_i$ means the Cholesky decomposition of S_i $(i = 1, 2)$
  $A \leftarrow \begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(1) & \mathrm{Tr}_{K/\mathbb{Q}}(\omega) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\omega) & \mathrm{Tr}_{K/\mathbb{Q}}(\omega^2) \end{pmatrix}$
  $B \leftarrow \begin{pmatrix} 1 & \ln|\epsilon_0^2| \\ 1 & \ln|\epsilon_0'^2| \end{pmatrix}$
- $L \leftarrow \Big\{(x_1, x_2)^t \in \mathcal{O}_K^2 \mid x_i = (x_{i1} + x_{i2}\omega),\ x_{i1}, x_{i2} \in \mathbb{Z}$ and $A[(x_{i1}, x_{i2})^t] \leq \frac{\alpha}{m},\ (i = 1, 2)\Big\}$
- $\mu \leftarrow \min_{x \in L} S[x]$
  For $x \in L$ do
  If $S[x] = \mu$ then $I \leftarrow I \cup \{x\}$
- For $x \in I$ do
  $k \leftarrow n \in \mathbb{Z}$ with $0 \leq \lambda_2 - n < 1$ where
  $\lambda = (\lambda_1, \lambda_2)^t \in \mathbb{R}^2$ with $B\lambda = \begin{pmatrix} \ln S_1[x] \\ \ln S_2[x'] \end{pmatrix}$
  $J \leftarrow J \cup \{x\epsilon^{-k}\}$
- Return J

3.4. Computing eutactic coefficients. For computing eutactic coefficients we use well known algorithms of combinatorics. There exist classical algorithms to compute barycentric coordinates based on linear programming.

4. Examples

Now we have the theoretical background and the algorithms for computing extreme Humbert forms. The algorithms are implemented in `KASH/KANT`. To continue we need the following lemma:

Lemma 15. *Let $S \in \mathcal{P}$ and $v_i = (\alpha, \beta)^t \in M(S)$ for $1 \leq i \leq s := |M(S)|$, and let v_{ij}, for $1 \leq i \neq j \leq s$, be the determinants of the correspnding pairs:*

$$v_{ij} = \det \begin{pmatrix} \alpha_i & \alpha_j \\ \beta_i & \beta_j \end{pmatrix}.$$

Then, for a fixed prime ideal $\mathfrak{p}$, with corresponding valuation $\nu_\mathfrak{p}$, we have: If $\{i, j, k\} \subseteq \{1, \ldots, s\}$ is ordered so that $\nu_\mathfrak{p}(v_{ij}) \geq \max(\nu_\mathfrak{p}(v_{ik}), \nu_\mathfrak{p}(v_{jk}))$, then

$$\nu_\mathfrak{p}(v_{ij}) \geq \nu_\mathfrak{p}(v_{ik}) = \nu_\mathfrak{p}(v_{jk}).$$

In particular, if $\{i, j\}$ is such that $\nu_\mathfrak{p}$ is maximal among all pairs $\{i, j\}$, we have

$$\nu_\mathfrak{p}(v_{ij}) \geq \nu_\mathfrak{p}(v_{ik}) = \nu_\mathfrak{p}(v_{jk})$$

for $k \neq i, j$.

Proof. For a proof see [BCIO] □

In the case $\mathbb{Q}(\sqrt{17})$ we are able to determine two extreme Humbert forms if we assume every extreme Humbert form has got a unimodular pair of minimal vectors. Of course these obtained extreme forms must not achieve the Hermite-Humbert constant for $\mathbb{Q}(\sqrt{17})$ but they are the first known examples of extreme Humbert forms for this number field.

With Algorithm 10 we compute 80436 triples. Now we solve polynomial equations to obtain Humbert forms and compute minimal vectors and if necessary eutactic coefficients. We give an example with the triple

$$\left\{ \begin{pmatrix} \frac{-5+\sqrt{17}}{2} \\ 1 \end{pmatrix}, \begin{pmatrix} \frac{-3+\sqrt{17}}{2} \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}.$$

If we write a Humbert form S as

$$S = \left(\begin{pmatrix} 1 & b_1 \\ b_1 & c \end{pmatrix}, \begin{pmatrix} 1 & b_2 \\ b_2 & c^{-1} \end{pmatrix} \right)$$

we obtain for every minimal vector $x = (x_1, x_2)^t \in \mathcal{O}_K^2$ polynomial equations in c, b_1 and b_2

$$S[x] - 1 = 0 \Leftrightarrow \left(x_1^2 + 2b_1 x_1 x_2 + c x_2^2\right)\left(c x_1'^2 + 2cb_2 x_1' x_2' + x_2'^2\right) - c = 0.$$

We use resultants of polynomials for eliminating b_1 and b_2 to obtain a polynomial in c like

$$f(c) = c^6 - \frac{3}{2}c^5 + \frac{-1360+330\sqrt{17}}{8}c^4 + \frac{2970-720\sqrt{17}}{4}c^3 + \frac{1360-330\sqrt{17}}{8}c^2 + \frac{-13062+3168\sqrt{17}}{4}c + \frac{4354-1056\sqrt{17}}{2}.$$

Now we obtain by factorizing

$$f(c) = \left(c^2 + \frac{16-4\sqrt{17}}{2}c + \frac{16\sqrt{17}-66}{2}\right) \cdot \left(c^2 + \frac{1-\sqrt{17}}{4}c + \frac{-9+\sqrt{17}}{8}\right) \cdot \left(c^2 + \frac{9\sqrt{17}-39}{4} + \frac{161-39\sqrt{17}}{8}\right)$$

and for $g(c) := c^2 + (8-2\sqrt{17})c + 8\sqrt{17} - 33$ we get

$$c_{1,2} = (\sqrt{17}-4) \pm \sqrt{2(33-8\sqrt{17})}.$$

Because of $(-4+\sqrt{17})^2 = 33 - 8\sqrt{17}$ the solutions $c_{1,2}$ are in the field $L := \mathbb{Q}(\sqrt{17}, \sqrt{2})$ and we obtain by $c > 0$

$$c = \sqrt{17} - 4 + \sqrt{2}\sqrt{17} - 4\sqrt{2}.$$

Then we fit c into the polynomial

$$\left(-(128+32\sqrt{17})c^2 - 16c\right) b_1^2 + \left((264+64\sqrt{17})c^3 + (64+20\sqrt{17})c^2 + 8c\right) b_1 + -(132+32\sqrt{17})c^4 - (68+16\sqrt{17})c^3 - (12+2\sqrt{17})c^2 + (32-8\sqrt{17})c$$

to obtain

$$b_1^2 + \left(\frac{13}{4} - \sqrt{17} + \sqrt{34} - \frac{17}{4}\sqrt{2}\right) b_1 + \left(\frac{\sqrt{17}}{2} - \frac{15}{8} + \frac{17\sqrt{2}}{8} - \frac{\sqrt{34}}{2}\right) = 0$$

which leads to $b_1 = \frac{1}{2}$. In a last step we fit these solutions into the polynomial

$$\left(8cb_1 - (5+\sqrt{17})c^2 + (-10+2\sqrt{17})c\right) b_2 + \left(-(10+2\sqrt{17})c + (-5+\sqrt{17})\right) b_1 + \frac{21+5\sqrt{17}}{2}c^2 + 4c + \frac{21-5\sqrt{17}}{2}$$

and obtain

$$(7\sqrt{17}-29)b_2 + \frac{29-7\sqrt{17}}{2} = 0$$

with $b_2 = \frac{1}{2}$. Now we get the following Humbert form $S = (S_1, S_2) =$

$$\left(\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & -4+\sqrt{17}-4\sqrt{2}+\sqrt{34} \end{pmatrix}, \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & -4-\sqrt{17}+4\sqrt{2}+\sqrt{34} \end{pmatrix}\right)$$

with $m(S) = 1$. For the eutactic coefficients we get

$$\rho_1 = \rho_2 = \rho_3 = \rho_4 = \tfrac{8+\sqrt{34}}{30}, \quad \rho_5 = \tfrac{14-2\sqrt{34}}{15}$$

and for the minimal vectors we compute $M(S)\backslash\{x_5 := e_1, x_3 := e_2\} =$

$$\left\{x_1 := \begin{pmatrix} \frac{-5+\sqrt{17}}{2} \\ 1 \end{pmatrix}, x_2 := \begin{pmatrix} \frac{-3+\sqrt{17}}{2} \\ -1 \end{pmatrix}, x_4 := \begin{pmatrix} 1 \\ -1 \end{pmatrix}\right\}.$$

Together we obtain

$$S^{-1} = \sum_{i=1}^{5} \rho_i \left(\frac{x_i x_i^t}{S_1[x]}, \frac{x_i' x_i'^t}{S_2[x']}\right)$$

and $\dim \sum_{X \in X_S} \mathbb{R}X$ is equal to 5. Finally we compute

$$\gamma_K(S) = 2.607989300\ldots$$

as a local maximum of γ_K.

In the same way we obtain an extreme Humbert form $S = (S_1, S_2) =$

$$\left(\begin{pmatrix} 1 & \frac{3+5\sqrt{17}-3\sqrt{5}-\sqrt{85}}{16} \\ \frac{3+5\sqrt{17}-3\sqrt{5}-\sqrt{85}}{16} & \frac{3-\sqrt{5}}{2} \end{pmatrix}, \begin{pmatrix} 1 & \frac{3-5\sqrt{17}+3\sqrt{5}-\sqrt{85}}{16} \\ \frac{3-5\sqrt{17}+3\sqrt{5}-\sqrt{85}}{16} & \frac{3+\sqrt{5}}{2} \end{pmatrix}\right)$$

with $m(S) = 1$. For the eutactic coefficients we get

$$\rho_1 = \frac{12}{45}, \quad \rho_2 = \frac{44-2\sqrt{85}}{45}, \quad \rho_3 = \frac{11+\sqrt{85}}{45}, \quad \rho_4 = \frac{12}{45} \quad \text{und } \rho_5 = \frac{11+\sqrt{85}}{45}$$

and for the minimal vectors we compute $M(S)\backslash\{x_5 := e_1, x_3 := e_2\}=$

$$\left\{x_1 := \begin{pmatrix} \frac{3-\sqrt{17}}{2} \\ 1 \end{pmatrix}, x_2 := \begin{pmatrix} \frac{5-\sqrt{17}}{2} \\ \frac{3-\sqrt{17}}{2} \end{pmatrix}, x_4 := \begin{pmatrix} 1 \\ \frac{-3-\sqrt{17}}{2} \end{pmatrix}\right\}.$$

Together we obtain

$$S^{-1} = \sum_{i=1}^{5} \rho_i \left(\frac{x_i x_i^t}{S_1[x]}, \frac{x_i' x_i'^t}{S_2[x']}\right)$$

and $\dim \sum_{X \in X_S} \mathbb{R}X$ is equal to 5. Finally We compute

$$\gamma_K(S) = 2.527919014\ldots$$

as a local maximum of γ_K.

Now we can use our algorithms to compute the Hermite-Humbert constant for the case $K = \mathbb{Q}(\sqrt{13})$. We need the following lemma:

Lemma 16. *If $K = \mathbb{Q}(\sqrt{13})$ and $\gamma_{K,2} \leq \frac{d_K}{2} = 6.5$ then any Humbert form S with more than 4 minimal vectors has got a unimodular pair of minimal vectors.*

Proof. Let assume there is no unimodular pair in $M(S)$. With the notations of lemma 15 we obtain $|\mathrm{N}_{K/\mathbb{Q}}(\det v_{ij})| \leq \gamma_{K,2}$ for each v_{ij} and there holds $\nu_{\mathfrak{p}_k}(v_{ij}) = 1$ for at least $k = 1, 2$ or $k = 3$ where $\mathfrak{p}_1 = (2)$ and $\mathfrak{p}_2\mathfrak{p}_3 = (3)$. Further only one of these prime ideals can divide each v_{ij} by lemma 15. Suppose this is done by the prime ideal $\mathfrak{p}_1$. Because of $e_1 \in M(S)$ we obtain $\nu_{\mathfrak{p}_1}(\beta) = 1$ for all $(\alpha, \beta)^t \in M(S)$. Now let $m_1 := (\alpha_1, \beta_1)^t, m_2 := (\alpha_2, \beta_2)^t \in M(S)$ and $M \in \mathrm{GL}(2, K)$ with columns m_1 and m_2. By assumption $\nu_{\mathfrak{p}_1}(\det M) = 1 = \nu_{\mathfrak{p}_1}(\alpha_1\beta_2 - \alpha_2\beta_1) = \nu_{\mathfrak{p}_1}(\gamma) + \nu_{\mathfrak{p}_1}(\alpha_1\epsilon_2 - \alpha_2\epsilon_1)$ with $\beta_i = (\gamma)\epsilon_i$ where $\nu_{\mathfrak{p}_1}(\gamma) = 1$ and $\epsilon_1, \epsilon_2 \in \mathcal{O}_K^\times$. Because of $|\mathcal{O}_K/\mathfrak{p}_1| = 4$ and $s \geq 5$ there muste be such $m_1, m_2 \in M(S)$ that $\nu_{\mathfrak{p}_1}(\alpha_1 - \alpha_2) > 0$, but then there holds $\nu_{\mathfrak{p}_1}(\alpha_1\epsilon_2 - \alpha_2\epsilon_1) > 0$, a contradiction.

□

By the algorithm 10 we obtain 3220 triples. Because of lemma 16 we know all extreme Humbert forms must have a unimodular pair of minimal vectors. We found 552 Humbert forms with more than 4 minimal vectors. By algorithm 11 we obtain 3 Humbert forms with more than four minimal vectors up to unimodular equivalence . Their minimal vectors are listed in the following table:

nr.	Minimal vectors without e_1 and e_2
1	$\begin{pmatrix} -3+\frac{1+\sqrt{13}}{2} \\ -2 \end{pmatrix}, \begin{pmatrix} -2+\frac{1+\sqrt{13}}{2} \\ -1+\frac{1+\sqrt{13}}{2} \end{pmatrix}, \begin{pmatrix} 1 \\ 1+\frac{1+\sqrt{13}}{2} \end{pmatrix}$
2	$\begin{pmatrix} -2+\frac{1+\sqrt{13}}{2} \\ -1+\frac{1+\sqrt{13}}{2} \end{pmatrix}, \begin{pmatrix} \frac{1+\sqrt{13}}{2} \\ 1+\frac{1+\sqrt{13}}{2} \end{pmatrix}, \begin{pmatrix} 1 \\ -1-\frac{1+\sqrt{13}}{2} \end{pmatrix}, \begin{pmatrix} 1 \\ 1+\frac{1+\sqrt{13}}{2} \end{pmatrix}$
3	$\begin{pmatrix} -3+\frac{1+\sqrt{13}}{2} \\ -2 \end{pmatrix}, \begin{pmatrix} -2+\frac{1+\sqrt{13}}{2} \\ -1+\frac{1+\sqrt{13}}{2} \end{pmatrix}, \begin{pmatrix} \frac{1+\sqrt{13}}{2} \\ 1+\frac{1+\sqrt{13}}{2} \end{pmatrix}, \begin{pmatrix} 2 \\ 2+\frac{1+\sqrt{13}}{2} \end{pmatrix}$

We obtain a critical Humbert form $S = (S_1, S_2)$ with

$$S_1 = \begin{pmatrix} 1 & \frac{-8+\sqrt{13}+7\sqrt{7}-2\sqrt{91}}{18} \\ \frac{-8+\sqrt{13}+7\sqrt{7}-2\sqrt{91}}{18} & \frac{7-2\sqrt{13}-14\sqrt{7}+4\sqrt{91}}{9} \end{pmatrix}$$

$$S_2 = \begin{pmatrix} 1 & \frac{-8-\sqrt{13}-7\sqrt{7}-2\sqrt{91}}{18} \\ \frac{-8-\sqrt{13}-7\sqrt{7}-2\sqrt{91}}{18} & \frac{7+2\sqrt{13}+14\sqrt{7}+4\sqrt{91}}{9} \end{pmatrix}.$$

with $m(S) = 1$. For its eutactic coefficients we compute

$$\rho_1 = \rho_2 = \tfrac{9+\sqrt{91}}{28}, \quad \rho_3 = \rho_6 = \tfrac{3(11-\sqrt{91})}{70}, \quad \rho_4 = \rho_5 = \tfrac{29+\sqrt{91}}{140}$$

and for its minimal vectors we get $M(S)\backslash\{x_3 := e_2, x_6 := e_1\} =$

$$\left\{ x_1 = \begin{pmatrix} \frac{-3+\sqrt{13}}{2} \\ \frac{-1+\sqrt{13}}{2} \end{pmatrix}, \; x_2 = \begin{pmatrix} \frac{1+\sqrt{13}}{2} \\ \frac{3+\sqrt{13}}{2} \end{pmatrix}, \; x_4 = \begin{pmatrix} 1 \\ -\frac{3+\sqrt{13}}{2} \end{pmatrix}, \; x_5 = \begin{pmatrix} 1 \\ \frac{3+\sqrt{13}}{2} \end{pmatrix} \right\}.$$

After verifying

$$S^{-1} = \sum_{i=1}^{6} \rho_i \left(\frac{x_i x_i^t}{S_1[x]}, \frac{x_i' x_i'^t}{S_2[x']} \right)$$

and $\dim \sum_{X \in X_S} \mathbb{R}X$ is equal to 5, we get

$$\gamma_K(S) = \gamma_{K,2} = 4.0353243\ldots$$

because of S is critical.

Aknowledgement: We thank the referee for various insightful comments.

References

[H] P. Humbert, *Théorie de la réduction des formes quadratique définies positives dans un corps algébrique K fini.* Comment. Math. Helv. **12** (1940), 263–306.

[BCIO] R. Baeza, R. Coulangeon, M.I. Icaza and M. O' Ryan, *Hermite's constant for quadratic number fields.* Experimental Mathematics **10** (2001), 543–551.

[C] R. Coulangeon, *Voronoï theory over algebraic number fields.* Monographies de l'Enseignement Mathématique **37** (2001), 147–162.

[Co1] H. Cohn, *A numerical survey of the floors of various Hilbert fundamental domains* Math. Comp. **19** (1965), 594–605. b

[Co2] H. Cohn, *On the shape of the fundamental domain of the Hilbert modular group* Proc. Symp. Pure Math. **8** (1965), 190–202.

[Ica] M.I. Icaza, *Hermite constant and extreme forms for algebraic number fields* J. London Math. Soc. **55** (1997), 11–22.

Marcus Wagner
Technische Universität Berlin
Fakultät II
Institut für Mathematik MA 8-1
Str. d. 17. Juni 136

D-10623 Berlin
Germany

E-mail : wagner@math.tu-berlin.de

Michael E. POHST
Technische Universität Berlin
Fakultät II
Institut für Mathematik MA 8-1
Str. d. 17. Juni 136
D-10623 Berlin
Germany

E-mail : pohst@math.tu-berlin.de