Hermite's Constant for Quadratic Number Fields

Ricardo Baeza, Renaud Coulangeon, Maria Ines Icaza, and Manuel O'Ryan

CONTENTS

We develop a method to compute the Hermite-Humbert constants $\gamma_{K,n}$ of a real quadratic number field K, the analogue of the classical Hermite constant γ_n when $\mathbb{Q}$ is replaced by a quadratic extension. In the case n = 2, the problem is equivalent to the determination of lowest points of fundamental domains in $\mathbb{H}^2$ for the Hilbert modular group over K, that had been studied experimentally by H. Cohn. We establish the results he conjectured for the fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$. The method relies on the characterization of extreme forms in terms of perfection and eutaxy given by the second author in an earlier paper.

1. INTRODUCTION

Let $K/\mathbb{Q}$ be a quadratic totally real number field, with ring of integers $\mathcal{O}_K$ and discriminant d_K. Let $S = (S_1, S_2)$ be a binary Humbert form over K [Baeza and Icaza 1997; Icaza 1997], i.e., S_1, S_2 are positive definite 2×2 real symmetric matrices. We denote by $\mathbf{P} \subset \mathbb{R}^6$ the space of such forms. The group $\mathrm{GL}(2, \mathcal{O}_K)$ of invertible 2×2 matrices with entries in the ring of integers $\mathcal{O}_K$ of K acts on $\mathbf{P}$: if $U \in \mathrm{GL}(2, \mathcal{O}_K)$ and $U^{(1)}, U^{(2)}$ denote the images of U under the 2 distinct embeddings of $\mathrm{GL}(2, \mathcal{O}_K)$ in $\mathrm{GL}(2, \mathbb{R})$, then $S[U] = (S_1[U^{(1)}], S_2[U^{(2)}])$, where $A[B]$ means $B^t AB$ whenever the product is defined. The set of forms $\{S[U] : U \in \mathrm{GL}(2, \mathcal{O}_K)\}$ is the equivalence class of S. If $u \in \mathcal{O}_K^2$, we define the value of S at u by $S[u] = S_1[u^{(1)}]S_2[u^{(2)}]$, and the *minimum* of S is then

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

Let $\det S = \det S_1 \det S_2$. Then $\det S$ as well as $m(S)$ are class invariants of S, and we obtain the class-invariant function

$$\gamma_K : \mathbf{P} \longrightarrow \mathbb{R}_{>0}, \quad \gamma_K(S) = \frac{m(S)}{(\det S)^{1/2}}. \tag{1–1}$$

This function is bounded by the constant $(\frac{\pi}{4})^2|\mathrm{d}_K|$ [Icaza 1997]. Actually Cohn has shown that $\frac{1}{2}|\mathrm{d}_K|$ is a bound for γ_K (see [Cohn 1965b] or [Ohno and

Baeza was partially supported by Fondecyt grant 1970214 and P. Formas cuadraticas, U. de Talca. Coulangeon was partially supported by European Union grant #CI1*-CT93-0353. Icaza and O'Ryan were partially supported by Fondecyt grant 1990897 and P. Formas cuadraticas, U. de Talca.

1058-6458/2001 $0.50 per page

Watanabe 2001] for a generalised version). Thus one can define the generalized Hermite constant of K (for binary forms)

$$\gamma_{K,2} = \sup_{S \in \mathbf{P}} \gamma_K(S) \tag{1–2}$$

The aim of this paper is to compute $\gamma_{K,2}$ for the fields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$, as well as to obtain general results towards the computation of $\gamma_{K,2}$. This problem has been studied by H. Cohn [1965a; 1965b] under a different point of view. We now briefly relate $\gamma_{K,2}$ to Cohn's work on lowest points of fundamental domains in $\mathbb{H}^2$ for the action of $\mathrm{SL}(2, \mathcal{O}_K)$, where $\mathbb{H}$ denotes the upper half plane $\{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

If $\lambda = (\lambda_1, \lambda_2) \in \mathbb{R}_{>0} \times \mathbb{R}_{>0}$, it is clear that $\gamma_K(\lambda \cdot S) = \gamma_K(S)$, where $\lambda \cdot S = (\lambda_1 S_1, \lambda_2 S_2)$. This invariance of γ_K together with its class-invariance induces a function $\gamma_K : \mathbb{R}^2_{>0} \backslash \mathbf{P} / \mathrm{SL}(2, \mathcal{O}_K) \longrightarrow \mathbb{R}_{>0}$. Identifying $\mathbb{R}^2_{>0} \backslash \mathbf{P}$ with $\mathbf{SP} = \{(S_1, S_2) \in \mathbf{P} : \det S_1 = \det S_2 = 1\}$, we see that $\gamma_{K,2} = \sup_{S \in \mathbf{SP}} m(S)$ and $\gamma_K : \mathbf{SP} \longrightarrow \mathbb{R}_{>0}$ is given by $\gamma_K = m(S)$. On the other hand, the group $\mathrm{SL}(2, \mathcal{O}_K)$ acts on $\mathbb{H}^2 = \mathbb{H} \times \mathbb{H}$ by Möbius transformations by the rule

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} (z_1, z_2) = \left(\frac{\alpha^{(1)} z_1 + \beta^{(1)}}{\gamma^{(1)} z_1 + \delta^{(1)}}, \frac{\alpha^{(2)} z_2 + \beta^{(2)}}{\gamma^{(2)} z_2 + \delta^{(2)}} \right),$$

and we obtain a bijection $\varphi : \mathbf{SP} / \mathrm{SL}(2, \mathcal{O}_K) \longrightarrow \mathbb{H}^2 / \mathrm{SL}(2, \mathcal{O}_K)$ given by: for any $S = (S_1, S_2) \in \mathbf{SP}$ write $S_j = A_j A_j^t$ with $A_j \in \mathrm{SL}(2, \mathbb{R}), j = 1, 2$. Then $\varphi(S)$ is the class of $(A_1^{-1} i, A_2^{-1} i)$ in $\mathbb{H}^2 / \mathrm{SL}(2, \mathcal{O}_K)$. More precisely, if

$$S_j = \begin{pmatrix} a_j & b_j \\ b_j & d_j \end{pmatrix}$$

for $j = 1, 2$, then

$$\varphi(S) = \text{class of } \left(\frac{-b_1 + i}{a_1}, \frac{-b_2 + i}{a_2} \right).$$

Thus we have a function $\tilde{\gamma}_K : \mathbb{H}^2 \longrightarrow \mathbb{R}_{>0}$ which on $\mathbb{H}^2 / \mathrm{SL}(2, \mathcal{O}_K)$ is given by $\tilde{\gamma}_K = \gamma_K \circ \varphi^{-1}$. Now the relation of $\gamma_{K,2}$ with the lowest points of fundamental domains in $\mathbb{H}^2$ is clear. We assert that under certain hypothesis on the field K there exist fundamental domains $\mathbf{F} \subset \mathbb{H}^2$ for the action of $\mathrm{SL}(2, \mathcal{O}_K)$ such that

$$\tilde{\gamma}_K(z_1, z_2) = (y_1 y_2)^{-1} \tag{1–3}$$

for all $(z_1, z_2) \in \mathbf{F}$, where $y_j = \mathrm{Im}(z_j)$ for $j = 1, 2$.

In particular,

$$\gamma_{K,2} = \left(\inf_{(z_1, z_2) \in \mathbf{F}} (y_1 y_2) \right)^{-1} \tag{1–4}$$

The classical case $K = \mathbb{Q}$ illustrates this formula nicely. Any reduced positive definite binary form $S = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ satisfies $0 \leq 2b \leq a \leq c$ and $a = m(S)$. The corresponding point $\varphi(S) = z_S \in \mathbb{H}$ is $z_S = -b/a + i/a \in \mathbf{F} = \left\{ z \in \mathbb{H} : -\frac{1}{2} \leq x \leq \frac{1}{2}, |z| \geq 1 \right\}$. Thus $\mathrm{Im}(z_S)^{-1} = a = m(S) = \gamma_{\mathbb{Q}}(S)$ and we obtain $\gamma_2 = (\inf_{z \in \mathbf{F}} y)^{-1}$. A closer look at $\mathbf{F}$ shows that $\inf_{z \in \mathbf{F}} y = \sqrt{3}/2$, so that $\gamma_2 = 2/\sqrt{3}$.

We now show assertion (1–3). We will assume that K has class number 1. Then any $S \in \mathbf{SP}$ is equivalent under $\mathrm{SL}(2, \mathcal{O}_K)$ to a form $S' = S[U]$ such that

$$m(S) = m(S') = S'[(1, 0)^t] = a_1 a_2.$$

This follows from the fact that all minimal vectors of S are unimodular [Baeza and Icaza 1997] and that one can transform such vectors into $(1, 0)$ by elements of $\mathrm{SL}(2, \mathcal{O}_K)$. Thus replacing S by S' we may assume $m(S) = S[(1, 0)^t] = a_1 a_2$, where $S = \left(\left(\begin{smallmatrix} a_1 & b_1 \\ b_1 & c_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} a_2 & b_2 \\ b_2 & c_2 \end{smallmatrix}\right) \right)$. Now $z_S = \varphi(S) \in \mathbb{H}^2$ is given by

$$(z_1, z_2) = \left(-\frac{b_1}{a_1} + \frac{1}{a_1} i, -\frac{b_2}{a_2} + \frac{1}{a_2} i \right),$$

and hence

$$\gamma_K(S) = m(S) = a_1 a_2 = (y_1 y_2)^{-1}.$$

This remark shows that we only need to look at fundamental domains in $\mathbf{SP}$ for $\mathrm{SL}(2, \mathcal{O}_K)$ where all elements S have the property that $(1, 0)$ is a minimal vector. Such fundamental domains can be constructed using Humbert's reduction theory [Humbert 1940]. The next result gives an explicit characterization of such domains.

For any $\alpha, \beta \in \mathcal{O}_K$ and $z = (z_1, z_2) \in \mathbb{H}^2$ let

$$\mathrm{N}_{\alpha,\beta}(z) = \left| \alpha^{(1)} z_1 + \beta^{(1)} \right|^2 \left| \alpha^{(2)} z_2 + \beta^{(2)} \right|^2$$

and define

$$\mathbf{F}_0 = \bigcap_{\substack{\alpha, \beta \in \mathcal{O}_K \\ \langle \alpha, \beta \rangle = \mathcal{O}_K}} \{ z \in \mathbb{H}^2 : \mathrm{N}_{\alpha,\beta}(z) \geq 1 \}, \tag{1–5}$$

where $\langle \alpha, \beta \rangle$ is the ideal generated by α and β.

Proposition 1.1. *Let $S \in \mathbf{SP}$ and let $z_S \in \mathbb{H}^2$ be the associated point in $\mathbb{H}^2$. The following assertions are equivalent*:

1. $\tilde{\gamma}_K(z_S) = (y_1 y_2)^{-1}$.

2. $m(S) = S[(1,0)^t]$.
3. $z_S \in \mathbf{F}_0$.

Proof. The equivalence between statements 1 and 2 follows from the discussion above. Next assume 2, so that $S[(\alpha,\beta)^t] \geq S[(1,0)^t]$ for all $\alpha,\beta \in \mathcal{O}_K$ with $(\alpha,\beta) \neq (0,0)$. Writing $S = \left(\left(\begin{smallmatrix} a_1 & b_1 \\ b_1 & c_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} a_2 & b_2 \\ b_2 & c_2 \end{smallmatrix}\right)\right)$, we get

$$\prod_{j=1}^{2}(a_j\alpha^{(j)2} + 2b_j\alpha^{(j)}\beta^{(j)} + c_j\beta^{(j)2}) \geq a_1a_2,$$

$$\prod_{j=1}^{2}(\alpha^{(j)2} + 2\frac{b_j}{a_j}\alpha^{(j)}\beta^{(j)} + \frac{c_j}{a_j}\beta^{(j)2}) \geq 1.$$

Since

$$z_S = \left(-\frac{b_1}{a_1} + i\frac{1}{a_1}, -\frac{b_2}{a_2} + i\frac{1}{a_2}\right),$$

we have

$$-\beta^{(j)}z_j + \alpha^{(j)} = \beta^{(j)}\frac{b_j}{a_j} + \alpha^{(j)} + \frac{\beta^{(j)}}{a_j}i,$$

and hence

$$\begin{aligned}
&\mathrm{N}_{-\beta,\alpha}(z_S) \\
&\quad = \left|-\beta^{(1)}z_1+\alpha^{(1)}\right|^2\left|-\beta^{(2)}z_2+\alpha^{(2)}\right|^2 \\
&\quad = \prod_{j=1}^{2}\left(\beta^{(j)^2}\left(\frac{b_j^2}{a_j^2}-\frac{1}{a_j^2}\right)+2\frac{b_j}{a_j}\alpha^{(j)}\beta^{(j)}+\alpha^{(j)2}\right) \\
&\quad = \prod_{j=1}^{2}\left(\alpha^{(j)2}+2\frac{b_j}{a_j}\alpha^{(j)}\beta^{(j)}+\frac{c_j}{a_j}\beta^{(j)2}\right) \geq 1,
\end{aligned}$$

because $b_j^2 - a_jc_j = 1$ for $j = 1,2$. This shows that $z_S \in \mathbf{F}_0$. Tracing back this computation, we see that statement 3 implies 2. □

Thus any fundamental domain $\mathbf{F}$ for $\mathrm{SL}(2,\mathcal{O}_K)$ in $\mathbb{H}^2$ contained in $\mathbf{F}_0$ satisfies $\gamma_{K,2} = (\inf_{z\in\mathbf{F}} y_1y_2)^{-1}$, establishing the relationship between the search for lowest points in such domains [Cohn 1965a; 1965b] and the search for extreme Humbert forms. We will in the next section stick to this last point of view. Our results (Section 3) will explain some of Cohn's computations and guesses. In Section 2 we will estimate the absolute values of the components of minimal vectors of Humbert forms. This will enable us to find a finite set of forms where we can expect to find extreme forms. To find them in this set, one uses the analogue of Voronoi's theory for number fields developed in [Coulangeon 2001]. In Section 3 we apply this strategy to compute $\gamma_{K,2}$ for the fields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$.

2. BOUNDS FOR MINIMAL VECTORS OF HUMBERT FORMS

Let $S \in \mathbf{P}$ be a binary Humbert form (S_1, S_2). Recall that a vector $u \in \mathcal{O}_K^2$ is minimal if $S[u] = m(S)$. If $\varepsilon \in U_k$ is a unit of K, then εu is also a minimal vector of S and the set $M(S)$ of classes of minimal vectors of S is finite [Icaza 1997]. Moreover, as in the classical case, it is known that if S is an extreme form, i.e., $\gamma_K(S)$ is a local maximum of γ_K, then the set $M(S)$ can not be too small. Using the characterization of extreme Humbert forms given in [Coulangeon 2001] we have:

Proposition 2.1. *If S is a perfect binary Humbert form over the totally real quadratic field K, then $|M(S)| \geq 5$.*

Proof. Recall that a perfect Humbert form S of rank n over a (totally real) field K of degree r is characterized by the condition

$$\dim_{\mathbb{R}} \sum_{u\in M(S)} \mathbb{R}u^tu = \frac{rn(n+1)}{2} - r + 1,$$

where u^tu is the vector

$$\left(\frac{u^{(1)t}u^{(1)}}{S_1[u^{(1)}]}, \ldots, \frac{u^{(r)t}u^{(r)}}{S_r[u^{(r)}]}\right);$$

see [Coulangeon 2001]. Thus in our case we obtain $\dim_{\mathbb{R}} \sum_{u\in M(S)} \mathbb{R}u^tu = 5$ and hence $|M(S)| \geq 5$. □

Remark 2.2. In terms of the associated points $z_S \in \mathbb{H}^2$, this result can be interpreted as follows: if $S \in \mathbf{SP}$ is extreme, then z_S lies at least on five hypersurfaces $\{\mathrm{N}_{\alpha,\beta}(z) = 1\}$ on the boundary of $\mathbf{F}_0$.

Proposition 2.1 now suggests the following procedure to find extreme Humbert forms. First note that after scaling a form S we can always assume $m(S) = 1$. The strategy then is roughly as follows:

1. Find a finite set $M_K \subset \mathcal{O}_K^2$ such that any extreme binary Humbert form is equivalent under $\mathrm{GL}(2,\mathcal{O}_K)$ to a form S with $|M(S) \cap M_K| \geq 5$.
2. For any 5-set $T = \{u_1, \ldots, u_5\} \subset M_K$ solve the linear equations in the unknown S

$$S[u_1] = \cdots = S[u_5] = 1.$$

3. Sort the resulting forms according to scaling $S \to \lambda S$, $\lambda \in \mathbb{R}^2_{>0}$ and integal equivalence $S \to S[U]$, for $U \in \mathrm{SL}(2, \mathcal{O}_K)$.
4. Test for perfection and eutaxy of the remaining forms using [Coulangeon 2001].

Theoretically the existence of the set M_K is assured by the reduction theory of P. Humbert [1940]. But unfortunately the description of the set of reduced Humbert forms involves unexplicit constants, which are difficult to estimate. The results in the next three lemmas will enable us to construct an explicit set M_K.

Lemma 2.3. *Let $S = (S_1, S_2) \in \mathbf{P}$, with*

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

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

$$\left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right| \leq \sqrt{\frac{c_1 c_2}{m(S)} \frac{S(u)}{m(S)}}\, \gamma_{K,2},$$

$$\left|\mathrm{N}_{K/\mathbb{Q}}(\beta)\right| \leq \sqrt{\frac{a_1 a_2}{m(S)} \frac{S(u)}{m(S)}}\, \gamma_{K,2},$$

$$\left|\alpha^{(1)}\beta^{(2)}\right| \leq \sqrt{\frac{a_2 c_1}{m(S)} \frac{S(u)}{m(S)}}\, \gamma_{K,2},$$

$$\left|\alpha^{(2)}\beta^{(1)}\right| \leq \sqrt{\frac{a_1 c_2}{m(S)} \frac{S(u)}{m(S)}}\, \gamma_{K,2}.$$

Proof. We have

$$\begin{aligned} S_i[u^{(i)}] &= a_i \alpha^{(i)^2} + c_i \beta^{(i)^2} + 2 b_i \alpha^{(i)} \beta^{(i)} \\ &= c_i \left(\beta^{(i)} + \frac{b_i}{c_i} \alpha^{(i)^2} + \frac{a_i c_i - b_i^2}{c_i} \alpha^{(i)^2} \right) \\ &\geq \frac{|S_i|}{c_i} \alpha^{(i)^2}, \end{aligned}$$

and the same inequality holds replacing α by β, and a_i by c_i respectively. The conclusion follows, writing $S(u) = S_1[u^{(1)}] S_2[u^{(2)}]$ in all four possible ways, and using

$$\frac{m(S)}{\sqrt{|S_1||S_2|}} \leq \gamma_{K,2}. \qquad \square$$

Lemma 2.4. *Let $u = {}^t(\alpha, \beta)$ and $v = {}^t(\nu, \mu) \in \mathcal{O}_K^2$ be minimal vectors of S, with $v \notin \mathcal{O}_K^\times u$, and $U = \left(\begin{smallmatrix} \alpha & \beta \\ \nu & \mu \end{smallmatrix}\right)$. Then*

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

Proof. Consider the Humbert form $S[U]$. Clearly, $m(S[U]) = m(S)$. On the other hand, $\det S[U] = \mathrm{N}_{K/\mathbb{Q}}(\det U)^2 \det S$, so that

$$\mathrm{N}_{K/\mathbb{Q}}(\det U)^2 = \frac{\det S[U]}{\det S}.$$

Now

$$\begin{aligned} \det S[U] &= \det S_1[U^{(1)}] \det S_2[U^{(2)}] \\ &\leq (S_1[u^{(1)}] S_1[v^{(1)}])(S_2[u^{(2)}] S_2[v^{(2)}]) \\ &= m(S)^2 = \det S \gamma_K(S)^2. \end{aligned}$$

Hence

$$\mathrm{N}_{K/\mathbb{Q}}(\det U)^2 \leq \gamma_K(S)^2 \leq \gamma_{K,2}^2. \qquad \square$$

As usual, we define *the* fundamental unit of K as the uniquely determined fundamental unit ε subject to the condition that $\varepsilon_0 = \varepsilon^{(1)} > 1$. We also define a constant C_K, depending only on K, as

$$C_K = \sup_{\eta = (\alpha, \beta) \in K^2} \inf_{u = (x,y) \in \mathcal{O}_K^2} \|\eta - u\|_\infty.$$

We also denote by $\{e_1, e_2\}$ the standard basis of $\mathcal{O}_K^2$.

Lemma 2.5. *If $h(K) = 1$, any binary Humbert form with at least 2 minimal vectors admits a representative $S = (S_1, S_2)$, modulo scaling and integral equivalence, such that*

1. *$m(S) = 1$, $e_1 \in M(S)$ and $S_1[e_1^{(1)}] = S_2[e_1^{(2)}] = 1$, so that*
$$S = \left(\begin{pmatrix} 1 & b_1 \\ b_1 & c_1 \end{pmatrix}, \begin{pmatrix} 1 & b_2 \\ b_2 & c_2 \end{pmatrix} \right).$$
2. *Any other minimal vector admits a representative $u = (x, y)^t$ modulo units satisfying*
$$|x^{(i)}| < \sqrt{\varepsilon_0 \gamma_{K,2}} (1 + C_K \varepsilon_0 \sqrt{\gamma_{K,2}}),$$
$$|y^{(i)}| < \varepsilon_0^{3/2} \gamma_{K,2}.$$

Proof. That one can assume that e_1 is minimal is clear since $h_K = 1$ and any minimal vector is primitive, i.e., its coordinates are coprime. The condition $S_1[e_1^{(1)}] = S_2[e_1^{(2)}] = 1$ is then easily fulfilled by scaling.

For the second assertion we proceed in several steps: first, let $u_2 = (x_2, y_2)$, with $y_2 \neq 0$, be a second minimal vector. We know from Lemma 2.4, applied to $U = \left(\begin{smallmatrix} 1 & x_2 \\ 0 & y_2 \end{smallmatrix}\right)$, that $\left|\mathrm{N}_{K/\mathbb{Q}}(y_2)\right| \leq \gamma_{K,2}$. Let $c_i' = A_i[u_2^{(i)}]$, for $i = 1, 2$. Since u_2 is minimal and we are assuming that $m(S) = 1$, we have $c_1' c_2' = 1$. Multiplying u_2 by a unit $\eta = \varepsilon^k$, $k \in \mathbb{Z}$,

changes c_1'/c_2' into $\varepsilon_0^{4k}c_1'/c_2'$, so we can assume that $\varepsilon_0^{-2} \le c_1'/c_2' < \varepsilon_0^2$, whence

$$\varepsilon_0^{-1} \le c_1' < \varepsilon_0,$$
$$\varepsilon_0^{-1} < c_2' \le \varepsilon_0.$$

Let $Y = \{y \in \mathcal{O}_K \setminus \{0\} : |\mathrm{N}_{K/\mathbb{Q}}(y)| \le \gamma_{K,2}\}$, and define $\bar{Y}$ to be the set of $y \in Y$ such that $\sqrt{\varepsilon_0^{-1}} \le |y^{(1)}| < \sqrt{\varepsilon_0\gamma_{K,2}}$ and $\sqrt{\varepsilon_0^{-1}} < |y^{(2)}| \le \sqrt{\varepsilon_0\gamma_{K,2}}$. This set is finite and any $y \in Y$ admits a representative modulo units in $\bar{Y}$. Thus, replacing S by $S[U]$ with $U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \eta \end{smallmatrix}\right)$, for a suitable unit η, one can assume that y_2 is in $\bar{Y}$ (indeed, replacing S by $S[U]$ amounts to replace e_2 by ηe_2, so y_2 is replaced by $\eta^{-1}y_2$, while x_2 remains unchanged).

We can moreover assume, replacing S by $S\left[\left(\begin{smallmatrix} 1 & q \\ 0 & 1 \end{smallmatrix}\right)\right]$ for a suitable $q \in \mathcal{O}_K$, that

$$|x_2^{(i)}| \le C_K y_2^{(i)}, \quad i = 1, 2.$$

Finally, let $u = (x, y)^t$ be any minimal vector; we show that, up to units, its coordinates can be bounded according to the lemma. We claim that there exists $\lambda \in \mathcal{O}_K$ with $\left|\mathrm{N}_{K/\mathbb{Q}}(\lambda)\right| \le \gamma_{K,2}$ such that $\lambda u \in \mathcal{O}_K e_1 \oplus \mathcal{O}_K u_2$, i.e.,

$$u = \frac{\tilde{x}}{\lambda}e_1 + \frac{\tilde{y}}{\lambda}u_2, \quad \tilde{x}, \tilde{y} \in \mathcal{O}_K. \tag{2–1}$$

The set choice of such λs is stable under multiplication by units, so we can assume without loss of generality that

$$\begin{aligned} \sqrt{\varepsilon_0^{-1}\left|\mathrm{N}_{K/\mathbb{Q}}(\lambda)\right|} \le |\lambda^{(1)}| < \sqrt{\varepsilon_0\left|\mathrm{N}_{K/\mathbb{Q}}(\lambda)\right|}, \\ \sqrt{\varepsilon_0^{-1}\left|\mathrm{N}_{K/\mathbb{Q}}(\lambda)\right|} < |\lambda^{(2)}| \le \sqrt{\varepsilon_0\left|\mathrm{N}_{K/\mathbb{Q}}(\lambda)\right|}, \end{aligned} \tag{2–2}$$

which allows a finite set of values for λ. Finally, having fixed $\lambda \in \mathcal{O}_K$ satisfying (2–1) and (2–2), we can still multiply u by a unit so as to have, for instance:

$$\begin{aligned} \sqrt{\varepsilon_0^{-1}\left|\mathrm{N}_{K/\mathbb{Q}}\left(\tilde{x}/\lambda\right)\right|} \le \left|\frac{\tilde{x}^{(1)}}{\lambda^{(1)}}\right| < \sqrt{\varepsilon_0\left|\mathrm{N}_{K/\mathbb{Q}}\left(\tilde{x}/\lambda\right)\right|}, \\ \sqrt{\varepsilon_0^{-1}\left|\mathrm{N}_{K/\mathbb{Q}}\left(\tilde{x}/\lambda\right)\right|} < \left|\frac{\tilde{x}^{(2)}}{\lambda^{(2)}}\right| \le \sqrt{\varepsilon_0\left|\mathrm{N}_{K/\mathbb{Q}}\left(\tilde{x}/\lambda\right)\right|}. \end{aligned} \tag{2–3}$$

Using Lemma 2.3, we infer that

$$\left|\mathrm{N}_{K/\mathbb{Q}}\left(\tilde{x}/\lambda\right)\right| \le \sqrt{c_1'c_2'}\gamma_{K,2} = \gamma_{K,2} \tag{2–4}$$

and that

$$\left.\begin{aligned} \left|\mathrm{N}_{K/\mathbb{Q}}\left(\tilde{y}/\lambda\right)\right| \le \gamma_{K,2}, \\ \left|\frac{\tilde{x}^{(1)}}{\lambda^{(1)}}\frac{\tilde{y}^{(2)}}{\lambda^{(2)}}\right| \le \sqrt{c_1'}\gamma_{K,2} < \sqrt{\varepsilon_0}\gamma_{K,2}, \\ \left|\frac{\tilde{x}^{(2)}}{\lambda^{(2)}}\frac{\tilde{y}^{(1)}}{\lambda^{(1)}}\right| \le \sqrt{c_2'}\gamma_{K,2} \le \sqrt{\varepsilon_0}\gamma_{K,2}. \end{aligned}\right\} \tag{2–5}$$

Clearly, λ being fixed, the set of $\tilde{x} \in \mathcal{O}_K$ satisfying (2–4) and (2–3) is finite, and then, inequalities (2–5) allow only a finite set of values for $\tilde{y}$. Going back to (2–1), we see that

$$|y^{(i)}| = \frac{|\tilde{y}^{(i)}|}{|\lambda^{(i)}|}|y_2^{(i)}|$$

is bounded, and that

$$|x^{(i)}| = \left|\frac{\tilde{x}^{(i)}}{\lambda^{(i)}} + \frac{\tilde{y}^{(i)}}{\lambda^{(i)}}x_2^{(i)}\right| \le \frac{|\tilde{x}^{(i)}|}{|\lambda^{(i)}|} + C_K\frac{|\tilde{y}^{(i)}|}{|\lambda^{(i)}|}|y_2^{(i)}|.$$

The explicit bounds of the lemma are then easily deduced from the various inequalities we have established. □

In some particular instances, the preceding lemma can be restated in a simpler way. We say that S admits a *unimodular pair* of minimal vectors if there exist $u, v \in M(S)$ such that $\mathcal{O}_K u \oplus \mathcal{O}_K v = \mathcal{O}_K^2$. Then:

Lemma 2.6. *If $h(K) = 1$, any Humbert form admitting a unimodular pair of minimal vectors is equivalent, up to scaling and integral equivalence, to a form*

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

with $\varepsilon_0^{-1} \le c < \varepsilon_0$. Moreover, $M(S) \supset \{e_1, e_2\}$ and any other minimal vector admits a representative $u = (x, y)^t$ modulo units satisfying

$$\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| \le \gamma_{K,2}, \quad \left|\mathrm{N}_{K/\mathbb{Q}}(y)\right| \le \gamma_{K,2} \tag{2–6}$$

and

$$|y^{(1)}| < \frac{\sqrt{\varepsilon_0}\gamma_{K,2}}{|x^{(2)}|}, \quad |y^{(2)}| \le \frac{\sqrt{\varepsilon_0}\gamma_{K,2}}{|x^{(1)}|}.$$

Proof. The assumption that S admits a unimodular pair allows to take $u_2 = e_2$ and $\lambda = 1$ in the proof of Lemma 2.5. The conclusion follows. □

Having explicitly described the set M_K, we can pass on to step 2 of the algorithm, that is solve the systems

$$S[u_1] = \cdots = S[u_5] = 1, \tag{2–7}$$

for all 5-sets $T = \{u_1, \ldots, u_5\}$ in M_K subject to the condition that any pair of vectors in T satisfies Lemma 2.4. According to Lemma 2.5, we can assume that $u_1 = e_1$, and write

$$S = \left(\begin{pmatrix} 1 & b_1 \\ b_1 & c_1 \end{pmatrix}, \begin{pmatrix} 1 & b_2 \\ b_2 & c_2 \end{pmatrix} \right).$$

So (2–7) is a system of polynomial equations in the 4 variables b_1, c_1, b_2, c_2 that we can solve using elimination theory (see the examples in the next section). When the condition of Lemma 2.6 is satisfied, we can assume that $u_2 = e_2$ and the number of variables reduces to three ($c_1 = c_2^{-1}$). Finally, since minimal vectors are defined up to multiplication by units, and $M(S[U]) = U^{-1}M(S)$ for any $U \in \mathrm{GL}(2, \mathcal{O}_K)$, we need to consider these different 5-sets in M_K only up to the following equivalence relation:

Definition 2.7. We call two 5-sets $\{u_1, \ldots, u_5\}$ and $\{v_1, \ldots, v_5\}$ of $\mathcal{O}_K^2$ equivalent if there exists $U \in \mathrm{GL}(2, \mathcal{O}_K)$ and $(\varepsilon_1, \ldots, \varepsilon_5) \in U_K^5$ such that

$$Uu_i = \varepsilon_i v_i, \quad i = 1, \ldots, 5.$$

This remark shortens notably the computations in the next section.

3. EXAMPLES

Let $K = \mathbb{Q}(\sqrt{d})$, with $d > 0$ a square free rational integer, and suppose that $h_K = 1$. As usual, we identify K with a subfield of $\mathbb{R}$, i.e., we fix an embedding of K, and we denote by x' the image of $x \in K$ by the nontrivial element of $Gal_{K/\mathbb{Q}}$.

As mentioned above, the computations are much more easy if one can restrict to forms admitting a unimodular pair of minimal vectors. It turns out that, for some small discriminants, one can show *a priori* that this condition will always hold for Humbert forms with sufficiently many minimal vectors — for example, perfect forms. This is based on observations of the following kind:

Lemma 3.1. *Let $S \in P_{2,K}$ and $v_i = (\alpha_i, \beta_i)^t \in M(S)$ for $1 \le i \le s$, and let $v_{i,j}$, for $1 \le i \ne j \le s$, be the determinants of the corresponding pairs*:

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

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

$$v_\mathfrak{p}(v_{i,j}) \ge v_\mathfrak{p}(v_{i,k}) = v_\mathfrak{p}(v_{j,k}).$$

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

$$v_\mathfrak{p}(v_{i,j}) \ge v_\mathfrak{p}(v_{i,k}) = v_\mathfrak{p}(v_{j,k}) \quad \text{for } k \ne i, j.$$

Proof. Expressing v_k as a linear combination, with coefficients in K, of v_i and v_j, we get

$$\begin{aligned} v_k = (\alpha_k, \beta_k) &= \frac{v_{k,i}}{v_{i,j}} v_i + \frac{v_{k,j}}{v_{j,i}} v_j \\ &= \left(\frac{v_{k,i}\alpha_i - v_{k,j}\alpha_j}{v_{i,j}}, \frac{v_{k,i}\beta_i - v_{k,j}\beta_j}{v_{i,j}} \right), \end{aligned}$$

and similarly permuting i, j and k. If $v_\mathfrak{p}(v_{i,j})$ were strictly less than both $v_\mathfrak{p}(v_{i,k})$ and $v_\mathfrak{p}(v_{j,k})$, then the valuation of α_k and β_k would be strictly positive, contradicting the primitivity of v_k. Thus

$$v_\mathfrak{p}(v_{i,j}) \ge \min(v_\mathfrak{p}(v_{i,k}), v_\mathfrak{p}(v_{j,k})),$$

and this holds for any permutation of i, j, k. This is easily seen to imply the assertion of the lemma. □

3A. K = $\mathbb{Q}(\sqrt{5})$

Beside Cohn's general upper bound $\gamma_{K,2} < d_K/2 = 2.5$, we can use in this case Götzky's estimate [1928]

$$\gamma_{\mathbb{Q}(\sqrt{5}),2} \le \frac{16}{-9 + \sqrt{312}} < 2.$$

Then Lemma 2.4 implies that any two noncolinear minimal vectors of $S \in \mathbf{P}$ generate $\mathcal{O}_K^2$, so Lemma 2.6 applies to any Humbert form S with $\#M(S) \ge 2$, and in particular to any perfect Humbert form. So we can restrict to forms

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

with $m(S) = 1$. The right-hand side of (2–6) is less than 2, and for the same reason as before, this implies that the coordinates of minimal vectors distinct from e_1 and e_2 are units. Up to multiplication by a suitable unit, we can assume that these

vectors are of the shape $(\alpha,1)^t$, with $\alpha \in U_K$, and Lemma 2.6 provides explicit bounds for α, namely $\alpha \in \{\pm 1, \pm\tau, \pm\tau'\}$, where $\tau = \frac{1}{2}(1+\sqrt{5})$. Finally, taking into account that each pair of minimal vectors has to satisfy Lemma 2.4, it is easily seen that, up to equivalence in the sense of Definition 2.7, the only 5-set to consider is

$$T = \{(1,0)^t,\ (0,1)^t,\ (1,1)^t,\ (\tau,1)^t,\ (-\tau',1)^t\}.$$

The requirement that vectors $u \in T$ satisfy $S(u)=1$ amounts to requiring that the following polynomials in c, b_1 and b_2 vanish simultaneously:

$$(1+2b_2)c^2 + (1+2b_2)(1+2b_1)c + (1+2b_1), \quad (3\text{–}1)$$

$$\tau'(\tau'+2b_2)c^2 - (\tau'+2b_2)(\tau+2b_1)c + \tau(\tau+2b_1), \quad (3\text{–}2)$$

$$\tau(-\tau+2b_2)c^2 + (-\tau+2b_2)(-\tau'+2b_1)c + \tau'(-\tau'+2b_1). \quad (3\text{–}3)$$

Eliminating b_2 between (3–1) $= 0$ and (3–2) $= 0$ yields

$$(8\tau c^2 + (8+8\tau)c)b_1^2 + ((4+4\tau)c^3 + 16\tau c^2 + (8+12\tau)c)b_1 + (2c^4 + (4+2\tau)c^3 + (2+6\tau)c^2 + (2+4\tau)c) = 0$$

and doing the same between (3–1) $= 0$ and (3–3) $= 0$ yields

$$((8+8\tau)c^2 + 8\tau c)b_1^2 + ((8+12\tau)c^3 + 16\tau c^2 + (4+4\tau)c)b_1 + ((2+4\tau)c^4 + (2+6\tau)c^3 + (4+2\tau)c^2 + 2c) = 0.$$

Finally, eliminating b_1 between these two equations, we find that c has to satisfy

$$c^5(c-1)^2(c-\tau^4)(c-\tau'^4)(c^2+3c+1) = 0, \quad (3\text{–}4)$$

whence $c = 1$, τ^2 or τ'^2. If one substitutes the value $c = 1$ into (3–2) and (3–3), the two equations are easily seen to be equivalent, so the initial system eventually reduces to the system

$$(1+2b_2) + (1+2b_2)(1+2b_1) + (1+2b_1) = 0,$$
$$\tau'(\tau'+2b_2) - (\tau'+2b_2)(\tau+2b_1) + \tau(\tau+2b_1) = 0.$$

Using the conditions $1 - b_i^2 > 0$ ($A_i > 0$), calculation yields $(b_1,b_2) = (-\frac{1}{2}\tau, -\frac{1}{2}\tau')$ or $(\frac{1}{2}\tau', \frac{1}{2}\tau)$. It is then easily checked that substituting $c = \tau^2$ or τ'^2 in (3–1)–(3–3) leads to equivalent solutions modulo integral equivalence. Thus, we have shown that the only possible perfect binary forms over $\mathbb{Q}(\sqrt{5})$ are

$$\mathcal{S} = \left(\begin{pmatrix} 1 & -\frac{1}{2}\tau \\ -\frac{1}{2}\tau & 1 \end{pmatrix}, \begin{pmatrix} 1 & -\frac{1}{2}\tau' \\ -\frac{1}{2}\tau' & 1 \end{pmatrix} \right)$$

and

$$\mathcal{S}' = \left(\begin{pmatrix} 1 & \frac{1}{2}\tau' \\ \frac{1}{2}\tau' & 1 \end{pmatrix}, \begin{pmatrix} 1 & \frac{1}{2}\tau \\ \frac{1}{2}\tau & 1 \end{pmatrix} \right).$$

But the two are equivalent:

$$\mathcal{S}' = \tau^{-2} \cdot \mathcal{S}\left[\begin{pmatrix} -1+\tau & -1+\tau \\ 0 & 1 \end{pmatrix} \right].$$

Since we know from [Coulangeon 2001] that there always exists at least one perfect form and at least one eutactic form, we conclude that $\mathcal{S}$ is perfect and eutactic. This can of course also be checked using the original definitions. Thus:

Theorem 3.2. *Up to scaling and equivalence under* $\mathrm{GL}(2,\mathcal{O}_K)$, *the form* $\mathcal{S}$ *is the only binary perfect Humbert form over* $\mathbb{Q}(\sqrt{5})$. *It has* $\#M(\mathcal{S}) = 5$ *minimal vectors, and is moreover eutactic, hence extreme. Consequently*

$$\gamma_{\mathbb{Q}(\sqrt{5}),2} = \gamma(\mathcal{S}) = \frac{4}{\sqrt{5}}.$$

3B. K = $\mathbb{Q}(\sqrt{2})$

In this case we can again apply Lemma 2.6, thanks to the following lemma:

Lemma 3.3. *Any binary Humbert form* S *over* $\mathbb{Q}(\sqrt{2})$ *with* $\#M(S) \geq 3$ *admits a unimodular pair.*

Proof. We let $\#M(S) = \{v_1, \ldots, v_s\}$, $s \geq 3$, and use the notation $v_{i,j}$ for the determinants of the various pairs, as in Lemma 3.1. Assume that no pair is unimodular, i.e., none of the $v_{i,j}$ is a unit. From Lemma 2.4, using the bound $\gamma_{K,2} < |d_K|/2 = 4$, we see that the only possible prime divisor for $v_{i,j}$ is $\mathfrak{p} = \sqrt{2}\mathcal{O}_K$, and that all $v_{i,j}$ must satisfy $v_{\mathfrak{p}}(v_{i,j}) = 1$. Without loss of generality, we can assume that $v_1 = (1,0)^t$. Writing $v_i = (\alpha_i, \beta_i)^t$, and multiplying each v_i by a suitable unit, we can therefore assume that $\beta_i = \sqrt{2}$ for $2 \leq i \leq s$. The v_i being primitive, we moreover have that $v_{\mathfrak{p}}(\alpha_i) = 0$, $2 \leq i \leq s$. Now the condition $v_{\mathfrak{p}}(v_{i,j}) = 1$, for $2 \leq i < j \leq s$ reads $v_{\mathfrak{p}}(\alpha_i - \alpha_j) = 0 = v_{\mathfrak{p}}(\alpha_i) = v_{\mathfrak{p}}(\alpha_j)$, which is impossible ($\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_2$). So at least one $v_{i,j}$ is a unit. □

We used PARI to classify all 5-sets of vectors satisfying Lemmas 2.3, 2.4 and 2.6 according to the equivalence relation of Definition 2.7. There are two

inequivalent sets to consider:

$$T_1=\{(1,0)^t,(0,1)^t,(-1-\sqrt{2},1)^t,(-\sqrt{2},1)^t,(-1,1)^t\},$$
$$T_2=\{(1,0)^t,(0,1)^t,(-1-\sqrt{2},1)^t,(-\sqrt{2},1)^t,(1,1)^t\}.$$

They correspond each to a system of polynomial equations, analogous to the system of the previous section given by the vanishing of (3–1)–(3–3). As before, we eliminate successively b_2 and b_1 and factorize over K the resulting polynomial in c, to find that c has to satisfy

$$\begin{aligned}\left(c^2-(2+\sqrt{2})c+3+2\sqrt{2}\right)&\\ \times\left(c^2-(1+\sqrt{2})c-(3+2\sqrt{2})\right)&\\ \times\left(c^2-\sqrt{2}c-1\right)=0&\end{aligned}\tag{3–5}$$

in the case of T_1, or

$$\begin{aligned}\left(c^4-(10+4\sqrt{2})c^3+(4+4\sqrt{2})c^2\right.&\\ \left.+(14+8\sqrt{2})c-(3+2\sqrt{2})\right)&\\ \times\left(c^2+(1+\sqrt{2})c-(3+2\sqrt{2})\right)=0.&\end{aligned}\tag{3–6}$$

in the case of T_2.

One can compute the real positive roots of these equations, substitute these values of c in the initial system, and then solve the corresponding systems in b_1 and b_2. Afterwards, one has to check that the resulting form are positive definite, and that their minimum is 1. In the case of T_1 and equation (3–5), the only root that leads to a Humbert form is $\frac{\sqrt{6}+\sqrt{2}}{2}$, the positive root of $c^2-\sqrt{2}c-1$, and the corresponding form is

$$\mathcal{S}_1=\left(\begin{pmatrix}1&\frac{1+\sqrt{2}}{2}\\ \frac{1+\sqrt{2}}{2}&\frac{\sqrt{6}+\sqrt{2}}{2}\end{pmatrix},\begin{pmatrix}1&\frac{1-\sqrt{2}}{2}\\ \frac{1-\sqrt{2}}{2}&\frac{\sqrt{6}-\sqrt{2}}{2}\end{pmatrix}\right).$$

In the case of T_2 and equation (3–6), the only root that leads to a Humbert form is $\frac{1+\sqrt{2}}{2}(\sqrt{5}-1)$ (positive root of $c^2+(1+\sqrt{2})c-(3+2\sqrt{2})$), the corresponding form being

$$\mathcal{S}_2=\left(\begin{pmatrix}1&\frac{\sqrt{2}}{2}\\ \frac{\sqrt{2}}{2}&\frac{(1+\sqrt{2})(\sqrt{5}-1)}{2}\end{pmatrix},\begin{pmatrix}1&\frac{-\sqrt{2}}{2}\\ \frac{-\sqrt{2}}{2}&\frac{(1-\sqrt{2})(\sqrt{5}+1)}{2}\end{pmatrix}\right).$$

But it is readily checked that $m(\mathcal{S}_2)<1$; for instance, $\mathcal{S}_2([2+\sqrt{2},-1-\sqrt{2}])=7-2\sqrt{10}<1$. Thus:

Theorem 3.4. *Up to scaling and equivalence under* $\mathrm{GL}(2,\mathcal{O}_K)$, *the form* $\mathcal{S}_1$ *is the only binary perfect Humbert form over* $\mathbb{Q}(\sqrt{2})$. *It has* $\#M(\mathcal{S}_1)=5$ *minimal vectors, and is eutactic, hence extreme. Consequently*

$$\gamma_{\mathbb{Q}(\sqrt{2}),2}=\gamma(\mathcal{S}_1)=\frac{4}{2\sqrt{6}-3}.$$

3C. K = $\mathbb{Q}(\sqrt{3})$

Lemma 3.5. *Any binary Humbert form* S *over* $\mathbb{Q}(\sqrt{3})$ *with* $\#M(S)\geq 5$ *admits a unimodular pair.*

Proof. We use the same notation as in the previous subsection and assume that none of the $v_{i,j}$ is a unit. Thanks to Lemma 2.4 and to the bound

$$\gamma_{K,2}<\tfrac{1}{2}|d_K|=6,\tag{3–7}$$

the only possible prime divisors for the $v_{i,j}$ are $\mathfrak{p}=\sqrt{3}\mathcal{O}_K$ and $\mathfrak{q}=(1-\sqrt{3})\mathcal{O}_K$. Moreover, a given $v_{i,j}$ cannot be divisible by both $\mathfrak{p}$ and $\mathfrak{q}$, since

$$\left|\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{pq})\right|=6>\gamma_{K,2}.$$

We claim that $\mathfrak{p}$ or $\mathfrak{q}$ has to divide all $v_{i,j}$ simultaneously. Suppose, for instance, that $\mathfrak{p}$ divides $v_{i,j}$. By Lemma 3.1, for any $k\neq i,j$, either $\mathfrak{p}$ divides both $v_{i,k}$ and $v_{j,k}$, or both have valuation 0. But in the second case, $v_{i,k}$ and $v_{j,k}$ would be divisible by $\mathfrak{q}$, and so would $v_{i,j}$, by Lemma 3.1 again. So $\mathfrak{pq}$ would divide $v_{i,j}$, which is impossible. The same holds replacing $\mathfrak{p}$ by $\mathfrak{q}$, which proves the claim. Let $m=\max_{i<j}v_{\mathfrak{q}}(v_{i,j})$. From Lemma 2.4 and bound (3–7), one has $m\leq 2$. If $m=0$, then all $v_{i,j}$ are divisible by $\mathfrak{p}$, with valuation 1, and we easily derive a contradiction, arguing exactly as in Lemma 3.3. So we assume that $m\geq 1$. Due to the previous remarks, this implies that all $v_{i,j}$ are divisible by $\mathfrak{q}$. We claim that for a given i, and for $j\neq k$ one cannot have $v_{\mathfrak{q}}(v_{i,j})=v_{\mathfrak{q}}(v_{i,k})=2$. Indeed, if such a triple $\{i,j,k\}$ existed, we could assume, up to a change of basis, that $v_i=(1,0)^t$ (since v_i is primitive), $v_j=(\alpha_j,\beta_j)^t$, $v_k=(\alpha_k,\beta_k)^t$, with $v_{\mathfrak{q}}(\beta_j)=v_{\mathfrak{q}}(\beta_k)=2$, and $v_{\mathfrak{q}}(\alpha_j)=v_{\mathfrak{q}}(\alpha_k)=0$ (primitivity of v_j and v_k). Scaling v_j and v_k by suitable units, we can moreover assume that $\beta_j=\beta_k$. Now the condition $v_{\mathfrak{p}}(v_{j,k})\leq 2$, implies $v_{\mathfrak{p}}(\alpha_k-\alpha_j)=0$, which is impossible ($\mathcal{O}_K/\mathfrak{q}\simeq\mathbb{F}_2$). Finally, assume, without loss of generality, that $v_1=(1,0)^t$. The previous observation, together with the assumption that $\mathfrak{q}$ divides all the $v_{i,j}$, and the fact that $\#M(S)\geq 5$, imply that $v_{\mathfrak{q}}(v_{1,j})=v_{\mathfrak{q}}(v_{1,k})=v_{\mathfrak{q}}(v_{1,l})=1$ for at least three distinct integers j, k, l, and that one of the pairs, say

$\{j,k\}$, satisfies $v_{\mathfrak{q}}(v_{j,k}) = 1$. Using the coordinates of v_j and v_k, scaled by suitable units, we conclude again that $v_{\mathfrak{q}}(\alpha_k) = v_{\mathfrak{q}}(\alpha_j) = v_{\mathfrak{q}}(\alpha_k - \alpha_j) = 0$, a contradiction. □

Here the classification of 5-sets of vectors satisfying Lemma 2.3, 2.4 and 2.6 is considerably more complicated. There are 37 such sets to consider, up to the equivalence relation of Definition 2.7. We solved the corresponding systems in the same way as in the previous subsections. Only 24 of them lead to actual Humbert forms i.e., positive definite. They fall into 2 distinct classes modulo integral equivalence and scaling, among which only one has minimum 1. This is obtained with the set

$$T_1' = \{(1,0)^t,\ (0,1)^t,\ (-u,\sqrt{3})^t,\ (-1-\sqrt{3},\sqrt{3})^t,\ (-u,1+\sqrt{3})^t\},$$

where $u = 2+\sqrt{3}$ is the fundamental unit of $\mathbb{Q}(\sqrt{3})$. The corresponding form is

$$\mathcal{S}_1' = \left(\begin{pmatrix} 1 & \frac{1}{2}u \\ \frac{1}{2}u & u \end{pmatrix}, \begin{pmatrix} 1 & \frac{1}{2}u' \\ \frac{1}{2}u' & u' \end{pmatrix}\right).$$

As in the case of $\mathbb{Q}(\sqrt{5})$, we can immediately conclude that it is both perfect and eutactic. It has $\#M(\mathcal{S}_1') = 12$ minimal vectors (up to units), given by

$$M(S_1') = \{(0,1)^t,\ (1,0)^t,\ (-u,\sqrt{3})^t, (-1-\sqrt{3},\sqrt{3})^t,\ (-3-2\sqrt{3},1+\sqrt{3})^t,\ (-u,1+\sqrt{3})^t,\ (-u,1)^t,\ (-2,1)^t,\ (-1-\sqrt{3},1)^t,\ (-1,1)^t,\ (-\sqrt{3},1)^t,\ (-u,2)^t\}.$$

Thus:

Theorem 3.6. *Up to scaling and equivalence under* $\mathrm{GL}(2,\mathcal{O}_K)$, *the form* $\mathcal{S}_1'$ *is the only binary perfect Humbert form over* $\mathbb{Q}(\sqrt{3})$. *It has* $\#M(\mathcal{S}_1') = 12$ *minimal vectors, and is eutactic, hence extreme. Consequently*

$$\gamma_{\mathbb{Q}(\sqrt{3}),2} = \gamma(\mathcal{S}_1') = 4.$$

REFERENCES

[Baeza and Icaza 1997] R. Baeza and M. I. Icaza, "On Humbert-Minkowski's constant for a number field", *Proc. Amer. Math. Soc.* **125**:11 (1997), 3195–3202.

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

[Cohn 1965b] H. Cohn, "On the shape of the fundamental domain of the Hilbert modular group", pp. 190–202 in *Theory of numbers*, edited by A. L. Whiteman, Proc. Symp. Pure Math. **8**, 1965.

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

[Götzky 1928] F. Götzky, "Über eine zahlentheoretische Anwendung von Modulfunktionen zweier Veränderlichen", *Math. Ann.* **100** (1928), 411–437.

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

[Icaza 1997] M. I. Icaza, "Hermite constant and extreme forms for algebraic number fields", *J. London Math. Soc.* (2) **55**:1 (1997), 11–22.

[Ohno and Watanabe 2001] S. Ohno and T. Watanabe, "Estimates of Hermite constants for algebraic number fields", *Comment. Math. Univ. St. Paul.* **50**:1 (2001), 53–63.

Ricardo Baeza, Instituto de Matemática y Física, Universidad de Talca, Casilla 721, Talca, Chile. (rbaeza@inst-mat.utalca.cl)

Renaud Coulangeon, Laboratoire A2X, Université Bordeaux I, 351 cours de la Libération, FR-33405, Talence, France (renaud.coulangeon@math.u-bordeaux.fr)

Maria Ines Icaza, Icaza, Instituto de Matemática y Física, Universidad de Talca, Casilla 747, Talca, Chile (icaza@inst-mat.utalca.cl)

Manuel O'Ryan, Icaza, Instituto de Matemática y Física, Universidad de Talca, Casilla 747, Talca, Chile (moryan@inst-mat.utalca.cl)

Received October 23, 2000; accepted in revised form March 29, 2001