Lenstra's Constant and Extreme Forms in Number Fields

R. Coulangeon, M. I. Icaza, and M. O'Ryan

CONTENTS

2000 AMS Subject Classification: 11H55

Keywords: Humbert forms, extreme forms

In this paper we compute $\gamma_{K,2}$ for $K = \mathbb{Q}(\rho)$, where ρ is the real root of the polynomial $x^3 - x^2 + 1 = 0$. We refine some techniques introduced in [Baeza et al. 01] to construct all possible sets of minimal vectors for perfect forms. These refinements include a relation between minimal vectors and the Lenstra constant. This construction gives rise to results that can be applied in several other cases.

1. INTRODUCTION

Let $K/\mathbb{Q}$ be a number field of degree $m = r+2s$, let d_K be its discriminant, and let $\mathcal{O}_K$ be its ring of integers. Let $\{\sigma_1, \ldots, \sigma_r\}$ (respectively $\{\sigma_{r+1}, \ldots, \sigma_m\}$ with $\sigma_{r+j} = \overline{\sigma}_{r+s+j}$) be its real (respectively complex) embeddings.

A tuple $S = (S_1, \ldots, S_{r+s})$, where $S_1, \ldots, S_r$ are n-dimensional real symmetric positive definite matrices and $S_{r+1}, \ldots, S_{r+s}$ are n-dimensional positive definite Hermitian matrices, is called an n-dimensional positive definite Humbert form. We refer to such forms as Humbert forms.

Following [Icaza 97], for a *column* vector $v = (a_1, \ldots, a_n)^t \in \mathcal{O}_K^n$ we define

$$S[v] = \prod_{i=1}^{r} S_i[v^{\sigma_i}] \Big(\prod_{i=r+1}^{r+s} S_i[v^{\sigma_i}] \Big)^2,$$

where $v^{\sigma_j} = (\sigma_j(a_1), \ldots, \sigma_j(a_n))^t$ for each embedding σ_j of K ($1 \leq j \leq r+s$) and $S_j[v^{\sigma_j}] := (v^{\sigma_j})^* S_j v^{\sigma_j}$. Here v^* denotes complex conjugation followed by transposition, i.e., $v^* = \overline{v}^t$.

The minimum of S is defined as

$$\mu(S) = \min_{v \in \mathcal{O}_K^n \setminus \{0\}} \left\{ \prod_{i=1}^{r} S_i[v^{\sigma_i}] \Big(\prod_{i=r+1}^{r+s} S_i[v^{\sigma_i}] \Big)^2 \right\}.$$

A vector $v \in \mathcal{O}_K^n \setminus \{0\}$ is called a *minimal vector of* S if $S[v] = \mu(S)$. For each Humbert form, the set of minimal vectors is finite up to multiplication by units. Throughout this paper we denote by $M(S)$ a (finite) set

1058-6458/2007 $0.50 per page

of representatives of the minimal vectors of S and we call it the set of minimal vectors of S.

The *determinant* $d(S)$ of S is defined as

$$d(S) = \prod_{i=1}^{r} \det S_i \prod_{i=r+1}^{r+s} (\det S_i)^2.$$

For a Humbert form S, its γ constant is defined as

$$\gamma(S) = \frac{\mu(S)}{\det(S)^{1/n}}$$

(see [Icaza 97]).

Two n-dimensional Humbert forms S and T are called *equivalent* if there exists $U \in \mathrm{GL}(n, \mathcal{O}_K)$ such that $T = S[U]$, where for $S = (S_1, \ldots, S_{r+s})$, $S[U] = (S_1[\sigma_1(U)], \ldots, S_{r+s}[\sigma_{r+s}(U)])$. Then obviously $\gamma(S)$ is class-invariant. It is also invariant by *scaling*, namely, if $T = (T_1, \ldots, T_{r+s})$, with $T_i = \lambda_i S_i$ for some positive real numbers λ_i, then $\gamma(T) = \gamma(S)$. Consequently, for our purpose, the forms we will be dealing with will always be considered up to $\mathrm{GL}(n, \mathcal{O}_K)$ equivalence and scaling.

The n-dimensional Hermite–Humbert constant of K is then given by (see [Icaza 97])

$$\gamma_{K,n} = \sup_S \gamma(S) = \sup_S \frac{\mu(S)}{d(S)^{1/n}},$$

where the supremum is taken over all n-dimensional positive definite Humbert forms S.

A form S that is a local maximum for $\gamma(S)$ is called an *extreme form*.

In a previous work by Baeza, Coulangeon, Icaza, and O'Ryan [Baeza et al. 01], the actual values for $\gamma_{K,2}$ were obtained for $K = \mathbb{Q}(\sqrt{5})$, $K = \mathbb{Q}(\sqrt{3})$, and $K = \mathbb{Q}(\sqrt{2})$. More recently, $\gamma_{K,2}$ for $K = \mathbb{Q}(\sqrt{13})$ was computed in [Pohst and Wagner 05].

In all those cases, the main computational tool was provided in [Coulangeon 01], which generalizes a result due to Voronoi, namely the characterization of *extreme forms* for the classical Hermite constant as forms that are perfect and eutactic. In his work, Coulangeon obtains the same characterization for *extreme forms* for the Hermite–Humbert constant by introducing suitable definitions for perfection and eutaxy. Considering this characterization, the procedure for finding perfect forms is based on the construction of their possible sets of minimal vectors (see [Baeza et al. 01]). Such a construction turns out to be not easy, and it becomes more complicated as the degree of the field or the dimension of the forms increases. The same strategy has been used to provide all known examples so far (see also [Pohst and Wagner 05]).

In Section 2 we show how this construction can be related to the so-called Lenstra constant of a number field K (see [Lenstra 97]). This constant, $L(K)$, defined for any number field, is the maximal length m of sequences $\omega_1, \ldots, \omega_m$ in $\mathcal{O}_K$ for which all possible mutual differences $\omega_i - \omega_j$ are units (we have not used the original notation $M(K)$ employed by Lenstra). Following [Leutbecher and Martinet 82], a sequence of the form $0 = \omega_1, 1 = \omega_2, \omega_3, \ldots, \omega_n$ of elements of K such that $\omega_i - \omega_j$ is a unit ($1 \le i < j \le n$) is called an *exceptional sequence*. A unit $u \in \mathcal{O}_K^*$ such that $1 - u$ is also a unit is called an *exceptional unit*.

In Section 3 we obtain $\gamma_{K,2}$ for the cubic field $K = \mathbb{Q}(\rho)$, where ρ is the real root of the polynomial $x^3 - x^2 + 1 = 0$. Finally, in Section 4 we give a list of other number fields in which the value of Lenstra's constant makes them suitable for applying the same techniques to obtain their binary Hermite–Humbert constant. We also provide in this last section some further remarks.

2. PRELIMINARY RESULTS

We begin this section by introducing some standard techniques from the geometry of numbers. We will define a fundamental domain X that will provide us with a suitable finite set of algebraic integers; see Definition 2.3.

Let K be a number field with $[K : \mathbb{Q}] = r + 2s$. Let $\sigma_1, \ldots, \sigma_r : K \to \mathbb{R}$ be the real embeddings of K and $\sigma_{r+1}, \ldots, \sigma_{r+s} : K \to \mathbb{C}$ the complex embeddings as described in the introduction. The *geometric representation* of K is the map $x : K \to \mathbb{R}^r \times \mathbb{C}^s$, $x(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r+s}(\alpha))$. If $\alpha \in K^*$, the image $x(\alpha)$ lies in $(\mathbb{R}^r \times \mathbb{C}^s)_* := \{x \in \mathbb{R}^r \times \mathbb{C}^s : x_i \neq 0 \text{ for } 1 \le i \le r+s\}$. In general, we identify $\mathbb{R}^r \times \mathbb{C}^s$ with $\mathbb{R}^{r+2s}$ as an $(r+2s)$-dimensional real vector space.

Let us define $\ell : (\mathbb{R}^r \times \mathbb{C}^s)_* \to \mathbb{R}^{r+s}$ by

$$\ell(x_1, \ldots, x_{r+s}) = \left(\log|x_1|, \ldots, \log|x_r|, \log|x_{r+1}|^2, \ldots, \log|x_{r+s}|^2\right).$$

Considering these two maps, we obtain ℓ_K, the *logarithmic representation* of K, where $\ell_K : K^* \to \mathbb{R}^{r+s}$ is given by $\ell_K(\alpha) = \ell(x(\alpha))$.

If $\{\varepsilon_1, \ldots, \varepsilon_{r+s-1}\}$ is a set of fundamental units of K, then setting $\ell^* = (1, \ldots, 1, 2, \ldots, 2)$, the vector with r ones and s twos in $\mathbb{R}^{r+s}$, we see that the set $\{\ell^*, \ell_K(\varepsilon_1), \ldots, \ell_K(\varepsilon_{r+s-1})\}$ is an $\mathbb{R}$-basis of $\mathbb{R}^{r+s}$.

Every $x \in (\mathbb{R}^r \times \mathbb{C}^s)_*$ determines unique numbers $\xi, \xi_1, \ldots, \xi_{r+s-1} \in \mathbb{R}$ given by $\ell(x) = \xi\ell^* + \xi_1\ell_K(\varepsilon_1) + \cdots + \xi_{r+s-1}\ell_K(\varepsilon_{r+s-1})$.

In $\mathbb{R}^{r+2s}$ we define the following cone:

$$X = \Big\{x \in (\mathbb{R}^r \times \mathbb{R}^{2s})_* \,:\, 0 \le \xi_i < 1\,;\\ 0 \le \arg x_1 < \frac{2\pi}{k}\Big\},$$

where the ξ_i are defined as above and if $r > 0$, the condition on the argument means that $x \ge 0$. Here k is the number of roots of unity in K.

According to [Borevich and Shafarevich 66, Lemma 1, Section 5.2], we have the following lemma.

Lemma 2.1. *Any $\in x \in (\mathbb{R}^r \times \mathbb{R}^{2s})_*$ has a unique representation $x = y \cdot x(\eta)$ with $y \in X$ and $\eta \in \mathcal{O}_K^*$, where the product in $\mathbb{R}^{r+2s}$ is defined componentwise.*

We then have the following corollary.

Corollary 2.2. *In every class of associated numbers of K^* there is one and only one number whose geometric representation lies in X.*

In order to prove the main result of this section, Proposition 2.9, we now introduce some technical definitions.

Definition 2.3. Given a nonzero natural number $c \in \mathbb{N}$, let us consider the following set of algebraic integers:

$$\mathcal{N}_K(c) = \{\alpha \in \mathcal{O}_K \,:\, (\sigma_1(\alpha), \ldots, \sigma_{r+s}(\alpha)) \in X\\ \text{and } 1 < |N_{K/\mathbb{Q}}(\alpha)| \le c\}.$$

It is easy to see that this set is finite. We denote its order by $n_K(c)$.

We will also make use of the following definition.

Definition 2.4. For each $0 \neq \alpha \in \mathcal{O}_K$ we set

$$L_\alpha(K) = \sup\{m : \omega_0, \ldots, \omega_m \in \mathcal{O}_K \text{ such that}\\ \omega_i - \omega_j = \alpha\varepsilon_{ij}, \text{ with } \varepsilon_{ij} \in \mathcal{O}_K^*\}.$$

The following remark, although straightforward, will be needed later.

Remark 2.5. Let $\{\omega_0, \ldots, \omega_m\}$ be elements of $\mathcal{O}_K$ such that $\omega_i - \omega_j = \alpha\varepsilon_{ij}$ with $0 \neq \alpha \in \mathcal{O}_K$ and $\varepsilon_{ij} \in \mathcal{O}_K^*$. The correspondence $\omega_i \mapsto \frac{\omega_i - \omega_0}{\omega_1 - \omega_0} := \tilde{\omega}_i$ gives rise to the sequence $\{0, \tilde{\omega}_1, \ldots, \tilde{\omega}_n\}$, which satisfies $\tilde{\omega}_i - \tilde{\omega}_j \in \mathcal{O}_K^*$. Therefore, the Lenstra constant $L(K)$ is equal to $L_\alpha(K)$.

Our next results are related to Humbert forms. We first recall (see [Coulangeon 01]) that if S is an n-dimensional perfect Humbert form and $M(S)$ is its set of minimal vectors, then $\sharp M(S)$, the number of minimal vectors of S, satisfies

$$\sharp M(S) \ge r\frac{n(n+1)}{2} + sn^2 - (r+s-1). \tag{2–1}$$

We make the following definition:

Definition 2.6. A Humbert form S has a *unimodular minimal n-tuple* if there exist $v_1, \ldots, v_n \in M(S)$ such that $\mathcal{O}_K v_1 + \cdots + \mathcal{O}_K v_n = \mathcal{O}_k^n$.

This definition leads to the following result.

Proposition 2.7. *If a Humbert form S has a unimodular minimal n-tuple, we may assume by changing the equivalence class of S that $\{e_1, \ldots, e_n\} \subseteq M(S)$. Here e_i denotes the column vector with 1's in the ith row and zero elsewhere.*

Proof: Suppose that the Humbert form S has a unimodular minimal n-tuple. Then there exists a matrix $U \in \mathrm{GL}(n, \mathcal{O}_K)$ that applies this n-tuple to the set $\{e_1, e_2, \ldots, e_n\}$. Changing S to the equivalent form $S[U]$ gives the desired result. □

Bounds for the norm of the determinant of the matrices built on minimal vectors of a Humbert form were established in [Baeza et al. 01, Lemma 2.4]. Although stated there only for totally real number fields, it is not difficult to see that these bounds hold for general number fields. For the sake of completeness, we restate this lemma (without proof) in the more general setting we will need later:

Lemma 2.8. *Let K be a number field and S an n-dimensional Humbert form over K. Assume that S admits n linearly independent minimal vectors $u_i = (u_{i1}, \ldots, u_{in})^t$, $1 \le i \le n$, and let $U = (u_{ij})_{1 \le i,j \le n}$ be the matrix whose columns are the minimal vectors. Then*

$$|N_{K/\mathbb{Q}}(\det U)| \le \gamma_{K,n}.$$

We denote by $N_{K/\mathbb{Q}}$ the absolute norm $N_{K/\mathbb{Q}} : K \longrightarrow \mathbb{Q}$.

The following proposition is the main result of this section. It relates the Lenstra constant $L(K)$ to the existence of unimodular minimal pairs for binary Humbert forms. We denote by $[x]$ the least-integer function.

Proposition 2.9. *Let K be a number field of degree $m = r + 2s$. Denote by t the number of elements of largest norm contained in $\mathcal{N}_K([\gamma_{K,2}])$. Let $S = (S_1, \ldots, S_{r+s})$ be a perfect binary Humbert form. Suppose $e_1 = (1,0)^t \in M(S)$ and that*

$$L(K)\left((n_K([\gamma_{K,2}]) - t)^2 + n_K([\gamma_{K,2}])\right) < 2r + 3s. \quad (2\text{–}2)$$

Then S has a unimodular minimal pair. Moreover, if the set $\mathcal{N}_K([\gamma_{K,2}])$ is empty, then S always has a unimodular minimal pair.

Proof: Let S be a binary Humbert form. Lemma 2.8 tells us that for $v_i = (\alpha_{i1}, \alpha_{i2})^t$, $v_j = (\alpha_{j1}, \alpha_{j2})^t \in M(S)$ with $v_i \neq \mu v_j$ and $\mu \in \mathcal{O}_K^*$, the following inequality holds:

$$\left| N_{K/\mathbb{Q}}\left(\det \begin{bmatrix} \alpha_{i1} & \alpha_{j1} \\ \alpha_{i2} & \alpha_{j2} \end{bmatrix}\right)\right| \leq [\gamma_{K,2}]. \quad (2\text{–}3)$$

Then, if $e_1 \in M(S)$, we have for $v_j = (\alpha_{j1}, \alpha_{j2})^t \in M(S)$, $v_j \neq e_1$, that

$$\left| N_{K/\mathbb{Q}}\left(\det \begin{bmatrix} 1 & \alpha_{j1} \\ 0 & \alpha_{j2} \end{bmatrix}\right)\right| = |N_{K/\mathbb{Q}}(\alpha_{j2})| \leq [\gamma_{K,2}].$$

Assume that for each $v_i = (\alpha_{i1}, \alpha_{i2})^t \in M(S)$, $v_i \neq e_1$, one has $\alpha_{i2} \notin \mathcal{O}_K^*$. We will count the possible number of second coordinates of the minimal vectors satisfying this condition.

The above inequality implies that $\alpha_{i2} = \varepsilon_i \tau$ for some $\tau \in \mathcal{O}_K$ satisfying $|N_{K/\mathbb{Q}}(\tau)| \leq [\gamma_{K,2}]$ and some $\varepsilon_i \in \mathcal{O}_K^*$. That is, $\tau \in \mathcal{N}_K([\gamma_{K,2}])$.

For each $\tau \in \mathcal{N}_K([\gamma_{K,2}])$ we define a subset of $M(S)$ as follows:

$$M_\tau(S) = \{(\alpha_{i1}, \alpha_{i2})^t \in M(S) : \alpha_{i2} = \tau\varepsilon_i, \varepsilon_i \in \mathcal{O}_K^*\}.$$

Scaling by units, we may assume that for each $v_i \in M_\tau(S)$, one has $\alpha_{i2} = \tau$.

For any two vectors in $M_\tau(S)$, we have

$$\det \begin{bmatrix} \alpha_{i1} & \alpha_{j1} \\ \tau & \tau \end{bmatrix} = \tau(\alpha_{i1} - \alpha_{j1}).$$

Since τ is not a unit and $|N_{K/\mathbb{Q}}(\tau) N_{K/\mathbb{Q}}(\alpha_{i1} - \alpha_{j1})| \leq [\gamma_{K,2}]$, inequality (2–3) implies that we have to consider two possible cases:

(i) $\alpha_{i1} - \alpha_{j1} = \delta\varepsilon_{ij}$, with $\delta \in \mathcal{N}_K([\gamma_{K,2}])$, ε_{ij} a unit, and $|N_{K/\mathbb{Q}}(\delta)| < [\gamma_{K,2}]$.

(ii) $\alpha_{i1} - \alpha_{j1} \in \mathcal{O}_K^*$.

Case (i): It is clear that δ does not have the largest norm among the elements of $\mathcal{N}_K([\gamma_{K,2}])$. The definition of Lenstra's constant $L(K)$ and the fact that $L_\delta(K) = L(K)$ imply that for a fixed $\tau \in \mathcal{N}_K([\gamma_{K,2}])$, there are at most

$$L(K)(n_K([\gamma_{K,2}]) - t)$$

minimal vectors from the contribution of this case.

It is clear that in case (ii), we obtain at most $L(K)$ minimal vectors.

Considering both cases, we obtain at most $L(K)(n_K([\gamma_{K,2}]) - t + 1)$ minimal vectors in $M_\tau(S)$ for each τ. Each $\tau \in \mathcal{N}_K([\gamma_{K,2}])$, except for the elements of largest norm in $\mathcal{N}_K([\gamma_{K,2}])$, leads to the above number of possible minimal vectors. After taking into account all possible nonunits τ, we have altogether at most $L(K)(n_K([\gamma_{K,2}]) - t + 1)(n_K([\gamma_{K,2}]) - t)$ possible minimal vectors for the Humbert form S.

Let us now consider the contribution of the elements of largest norm in $\mathcal{N}_K([\gamma_{K,2}])$. If η is such an element in $\mathcal{N}_K([\gamma_{K,2}])$, then any two $v_i = (\alpha_{i1}, \alpha_{i2})^t$ and $v_j = (\alpha_{j1}, \alpha_{j2})^t \in M_\eta(S)$ satisfy $\alpha_{i1} - \alpha_{j1} \in \mathcal{O}_K^*$. Hence we have at most $L(K)$ possible vectors.

Therefore, we obtain altogether at most $L(K)\left((n_K([\gamma_{K,2}]) - t)^2 + n_K([\gamma_{K,2}])\right)$ possible minimal vectors for S whose second coordinates are nonunits.

Now assume in addition that S is perfect. The bound (2–1) on the number of minimal vectors implies that S has at least $2r+3s+1$ minimal vectors. We are assuming that $e_1 = (1,0)^t$ is one of the minimal vectors of S, and therefore S must have at least $2r + 3s$ minimal vectors different from e_1. Equation (2–2) now implies that at least for one $v = (\alpha_{i1}, \alpha_{i2})^t \in M(S)$, $\alpha_{i2} \in \mathcal{O}_K^*$. Thus $\{e_1, v\}$ is a unimodular minimal pair for S.

Notice that if $\mathcal{N}_K([\gamma_{K,n}])$ is empty, then S always has a unimodular minimal pair. □

As an immediate consequence of the previous result we have the following proposition.

Proposition 2.10. *Let $S = (S_1, \ldots, S_{r+s})$ be a perfect binary Humbert form over K (as above). Assume that $e_1 = (1,0)^t \in M(S)$ and suppose that for any $\alpha, \beta \in \mathcal{N}_K([\gamma_{K,2}])$ one has $\alpha\beta \notin \mathcal{N}_K([\gamma_{K,2}])$. If $L(K)n_K([\gamma_{K,2}]) < 2r+3s$, then S has a unimodular minimal pair.*

Proof: The condition for $\alpha, \beta \in \mathcal{N}_K([\gamma_{K,2}])$, $\alpha\beta \notin \mathcal{N}_K([\gamma_{K,2}])$, implies that in the proof of the above proposition we have only to consider case (ii). The same counting argument leads to the result. □

Remark 2.11. As a final remark we mention here that the previous proposition together with some easy combinatorial arguments simplifies the proof of the existence of a unimodular pair of minimal vectors for the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ included in [Baeza et al. 01] and the field $\mathbb{Q}(\sqrt{13})$ from [Pohst and Wagner 05].

3. AN EXAMPLE OF COMPUTATION OF $\gamma_{K,2}$

Let ρ be the real root of the irreducible polynomial $x^3 - x^2 + 1 \in \mathbb{Z}[x]$. We denote by K the cubic number field $\mathbb{Q}(\rho)$. The discriminant of K is $d_K = -23$; its class number is given by $h_K = 1$; its signature is $(1,1)$; and its ring of integers is $\mathcal{O}_K = \mathbb{Z}[\rho]$. Our aim is to determine $\gamma_{K,2}$. To this end, we will make use of the results of the previous section. Let $S = (S_1, S_2)$ be a two-dimensional Humbert form, that is, S_1 is a positive definite 2×2 symmetric real matrix and S_2 is a positive definite 2×2 Hermitian complex matrix.

Lemma 3.1. *Every binary Humbert form S over K with $\#M(S) \geq 2$ has a unimodular pair.*

Proof: Since the class number of K is 1, we can always assume that $e_1 = (1,0)^t \in M(S)$ for any binary Humbert form S. Using the results of [Ohno and Watanabe 01], one can bound $\gamma_{K,2}$ in terms of d_K and the classical Hermite constant $\gamma_{\mathbb{Q},6} = \sqrt[6]{64/3}$, obtaining

$$\gamma_{K,2} \leq 23 \frac{\left(\sqrt[6]{64/3}\right)^3}{3^3} \leq 3.94.$$

Since 2 and 3 are inert in K, there are no elements of norm 2 or 3 in $\mathcal{O}_K$. Hence $\mathcal{N}_K([\gamma_{K,n}])$ is empty. Now Proposition 2.9 implies the lemma. □

This lemma applies in particular to perfect binary Humbert forms over K, since they have at least six minimal vectors, according to the bound (2–1). If S is such a form, then up to $\mathrm{GL}(2, \mathcal{O}_K)$ equivalence, we may assume from the previous lemma that $M(S)$ contains both $e_1 = (1,0)^t$ and $e_2 = (0,1)^t$, which we do from now on.

Proposition 3.2. *Let S be a perfect binary Humbert form over K. Then*

(i) *$\#M(S) = 6$.*

(ii) *Up to $\mathrm{GL}(2, \mathcal{O}_K)$ equivalence, one may assume that*

$$M(S) \supset \{e_1, e_2, e_1 + e_2\}.$$

If that is the case, then there exist exceptional units μ_4, μ_5, μ_6 such that $\{0, 1, \mu_4, \mu_5, \mu_6\}$ is an exceptional sequence, and $M(S) = \{v_1, \ldots, v_6\}$, with $v_1 = e_1$, $v_2 = e_2$, $v_3 = e_1 + e_2$, and $v_i = (1, \mu_i)^t$ for $4 \leq i \leq 6$.

Proof: We may assume that $M(S) \supset \{e_1, e_2\}$ and consequently write $M(S) = \{v_1, v_2, \ldots, v_N\}$ with $v_1 = e_1$, $v_2 = e_2$, and $N = \#M(S)$. For $i \geq 3$, write $v_i = (\alpha_{i1}, \alpha_{i2})^t$. Using Lemma 2.8, we infer that

$$|N_{K/\mathbb{Q}}(\alpha_{i1})| = \left| N_{K/\mathbb{Q}} \left(\det \begin{bmatrix} 0 & \alpha_{i1} \\ 1 & \alpha_{i2} \end{bmatrix} \right) \right| \leq \gamma_{K,2} \quad (3–1)$$

and

$$|N_{K/\mathbb{Q}}(\alpha_{i2})| = \left| N_{K/\mathbb{Q}} \left(\det \begin{bmatrix} 1 & \alpha_{i1} \\ 0 & \alpha_{i2} \end{bmatrix} \right) \right| \leq \gamma_{K,2}. \quad (3–2)$$

Since

$$\gamma_{K,2} \leq 3.94$$

and there are no elements in $\mathcal{O}_K$ with norm 2 or 3, the components of v_i are either units or 0, the last possibility being excluded since we are assuming that $v_i \neq e_1, e_2$. Consequently, we can assume, up to multiplication by a unit, that $v_i = (1, \mu_i)^t$ with $\mu_i \in \mathcal{O}_K^*$. Now applying Lemma 2.8 again to the matrices $\left[\begin{smallmatrix} 1 & 1 \\ \mu_i & \mu_j \end{smallmatrix}\right]$, we conclude that $\mu_i - \mu_j \in \mathcal{O}_K^*$ for $i \neq j$. In other words, the set $\{0, \mu_3, \mu_4, \mu_5, \ldots, \mu_N\}$ is an exceptional sequence, so that its cardinality $N - 1$ is at most 5. But we know that $N \geq 6$, since S is perfect, and thus $N = 6$, which proves (i). As for the second assertion, we can replace S by the equivalent form $S\left[\left[\begin{smallmatrix} 1 & 0 \\ 0 & \mu_3 \end{smallmatrix}\right]\right]$ and assume consequently that $v_3 = (1,1)^t$, whence the conclusion. □

Having established these facts, we see that the solution to our problem is now theoretically simple, since it relies essentially on the enumeration of the possible sequences $\{\mu_4, \mu_5, \mu_6\}$ such that $\{0, 1, \mu_4, \mu_5, \mu_6\}$ is an exceptional sequence. In particular, the μ_i's have to be exceptional units. The set of exceptional units $\widetilde{E_K}$ is finite (see [Lang60]), and moreover, it is explicitly known: according to [Nagell 64, Théorème 2],

$$\widetilde{E_K} = \{\rho, -\rho, \rho^{-1}, -\rho^{-1}, \rho^2, \rho^{-2}, -\rho^4, -\rho^{-4}, -\rho^3, \\ -\rho^{-3}, -\rho^5, -\rho^{-5}\}.$$

This gives rise to finitely many sets $\{\mu_4, \mu_5, \mu_6\}$ and accordingly to finitely many possible sets of minimal vectors $\{v_1, \ldots, v_6\}$ with $v_1 = e_1$, $v_2 = e_2$, and $v_3 = e_1 + e_2$. Next we look for potential Humbert forms S satisfying

$M(S) = \{v_1, \dots, v_6\}$, which we may further assume to have minimum 1. This amounts, for each of these sets, to solving the set of polynomial equations

$$S[v_1] = \cdots = S[v_6] = 1. \tag{3–3}$$

Finally, we use the same equivalence relation among sets of minimal vectors as in [Baeza et al. 01], which shortens the computations. Namely, two sets $\{u_1, \dots, u_6\}$ and $\{v_1, \dots, v_6\}$ are equivalent if (after a permutation of one of the sets) there exists $U \in \mathrm{GL}(2, \mathcal{O}_K)$ and $(\epsilon_1, \dots, \epsilon_6) \in {\mathcal{O}_K^*}^6$ such that

$$Uu_i = \epsilon_i v_i, \quad i = 1, \dots, 6,$$

and it is enough to solve the systems (3–3) corresponding to inequivalent sets, since we are looking for extreme forms up to $\mathrm{GL}(2, \mathcal{O}_K)$ equivalence.

All the computations were made using MAGMA. We found six inequivalent sets according to the above equivalence relation. We assume that these sets satisfy the conditions of Proposition 3.2. To describe them, it is enough to know the three exceptional units μ_4, μ_5, and μ_6 corresponding to the second coordinates of v_4, v_5, and v_6 respectively. The six possibilities we found are as follows:

$$\begin{aligned}
E_1 &= \left\{-\rho^2 + 1, -\rho^2 + \rho, -\rho^2 + \rho + 1\right\},\\
E_2 &= \left\{-\rho^2 + 1, -\rho^2 + \rho, -\rho + 1\right\},\\
E_3 &= \left\{\rho^2 - \rho, -\rho, -\rho + 1\right\},\\
E_4 &= \left\{\rho^2 - 2\rho + 2, -\rho^2 + \rho, -\rho^2 + 2\rho - 1\right\},\\
E_5 &= \left\{\rho, -\rho^2 + \rho, -\rho^2 + \rho + 1\right\},\\
E_6 &= \left\{\rho^2 - 2\rho + 2, \rho^2 - \rho + 1, -\rho^2 + 2\rho - 1\right\}.
\end{aligned}$$

For the explicit computation we note that we can express the complex roots of the defining polynomial $x^3 - x^2 + 1$ in terms of ρ as

$$\rho_2 := \frac{(1-\rho) + \sqrt{-3\rho^2 + 2\rho - 1}}{2}$$

and

$$\rho_3 := \frac{(1-\rho) - \sqrt{-3\rho^2 + 2\rho - 1}}{2} = -\rho_2 - \rho + 1.$$

All computations can be done in the Galois closure of K, which is the degree-six extension

$$L = K\left(\sqrt{-3\rho^2 + 2\rho - 1}\right) = \mathbb{Q}\left(\rho, \sqrt{-3\rho^2 + 2\rho - 1}\right).$$

Also, we can express the unknown real matrix S_1 and the unknown complex matrix S_2 as $S_1 = \left[\begin{smallmatrix} q_1 & x \\ x & z_1 \end{smallmatrix}\right]$ and $S_2 = \left[\begin{smallmatrix} q_2 & y\rho_2 + t\rho_3 \\ y\rho_3 + t\rho_2 & z_2 \end{smallmatrix}\right]$, where $q_1, q_2, x, y, t, z_1, z_2$ are indeterminates.

Furthermore, $q_1 q_2^2 = 1$, since we are assuming that e_1 is minimal. Thus, scaling S_1 and S_2 by q_1^{-1} and q_2^{-1} respectively, which affects neither the minimum of S nor its set of minimal vectors, one can assume that $q_1 = q_2 = 1$. Thus we are left with only five unknowns x, y, t, z_1, z_2 in the expression of S_1 and S_2. For each of the sets above we can write a set of equations given by $S[v] = S_1[v^{\sigma_1}] S_2[v^{\sigma_2}]^2 = 1$, where v is a minimal vector and σ_1, σ_2 are the real and complex embeddings.

For instance, considering E_3 we have the following equations:

$$\begin{aligned}
&\left[\begin{smallmatrix} 1 & \rho^2-\rho \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & x \\ x & z_1 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 \\ \rho^2-\rho \end{smallmatrix}\right]\\
&\quad \times \left(\left[\begin{smallmatrix} 1 & \rho\rho_2 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & y\rho_2+t\rho_3 \\ y\rho_3+t\rho_2 & z_2 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 \\ -\rho\rho_2-\rho^2+\rho \end{smallmatrix}\right]\right)^2 = 1,\\
&\left[\begin{smallmatrix} 1 & -\rho \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & x \\ x & z_1 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 \\ -\rho \end{smallmatrix}\right]\\
&\quad \times \left(\left[\begin{smallmatrix} 1 & \rho_2-\rho+1 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & y\rho_2+t\rho_3 \\ y\rho_3+t\rho_2 & z_2 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 \\ -\rho_2 \end{smallmatrix}\right]\right)^2 = 1,\\
&\left[\begin{smallmatrix} 1 & -\rho+1 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & x \\ x & z_1 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 \\ -\rho+1 \end{smallmatrix}\right]\\
&\quad \times \left(\left[\begin{smallmatrix} 1 & \rho_2+\rho \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & y\rho_2+t\rho_3 \\ y\rho_3+t\rho_2 & z_2 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 \\ -\rho_2+1 \end{smallmatrix}\right]\right)^2 = 1.
\end{aligned}$$

These together with the equations arising from the minimal vectors $e_2, e_1 + e_2$ give a set of five equations in five unknowns, which for E_3 are

$$\begin{aligned}
&(1 + 2(\rho^2 - \rho)x + (-\rho + 1)z_1)\\
&\quad \times (1 - 2y + (-\rho^2 + \rho + 1)t + \rho z_2)^2 = 1,\\
&(1 - 2\rho x + \rho^2 z_1)\\
&\quad \times (1 + (\rho^2 - 1)y - 2(\rho^2 - \rho)t + (\rho^2 - \rho)z_2)^2 = 1,\\
&(1 - 2(\rho - 1)x + (\rho - 1)^2 z_1)\\
&\quad \times (1 + (\rho^2 - \rho)y + (-2\rho^2 + \rho + 1)t + \rho^2 z_2)^2 = 1,\\
&(1 + 2x + z_1)(1 - (\rho - 1)(y + t) + z_2)^2 = 1,\\
&z_1 z_2^2 = 1.
\end{aligned}$$

In order to solve these systems of equations, first we computed a Gröbner basis for the ideal they define in the polynomial ring $K[x, y, t, z_1, z_2]$. Then using floating-point computations (setting $\rho \approx -0.754877666246692760049\ldots$) we looked for real solutions to the equations. Once we had solutions, we imposed the condition on the positivity of the determinant of S and we traced back these floating-point solutions to obtain the solutions, just one for each set:

For the set E_1 we have

$$\begin{aligned}
x &= -\tfrac{1}{2}(\rho + 1), \quad z_1 = \rho^2 - \rho + 1, \quad z_2 = \sqrt{1 - \rho^2},\\
t &= \tfrac{1}{23}(-4\rho^2 - 10\rho - 12) + \tfrac{1}{23}(-8\rho^2 + 3\rho - 1)\sqrt{1 - \rho^2},\\
y &= \tfrac{1}{23}(4\rho^2 - 13\rho - 11) + \tfrac{1}{23}(-15\rho^2 - 3\rho + 1)\sqrt{1 - \rho^2}.
\end{aligned}$$

For E_2,

$$x = -\tfrac{1}{2}, \quad z_1 = 1, \quad z_2 = 1,$$
$$t = \tfrac{1}{23}(-11\rho^2 + 7\rho - 10) + \tfrac{1}{23}\sqrt{29\rho^2 + 15\rho + 41},$$
$$y = \tfrac{1}{23}(-12\rho^2 - 7\rho + 10) - \tfrac{1}{23}\sqrt{29\rho^2 + 15\rho + 41}.$$

For E_3,

$$x = -\tfrac{1}{2}(\rho^2 + 1), \quad z_1 = -\rho, \quad z_2 = \sqrt{\rho^2 - \rho},$$
$$t = \tfrac{1}{23}(\rho^2 - 9\rho + 3) + \tfrac{1}{23}(-10\rho^2 - 2\rho - 7)\sqrt{\rho^2 - \rho},$$
$$y = \tfrac{1}{23}(-\rho^2 - 14\rho - 3) + \tfrac{1}{23}(-13\rho^2 + 2\rho + 7)\sqrt{\rho^2 - \rho}.$$

For E_4,

$$x = \tfrac{1}{2}(\rho^2 - 2\rho - 2), \quad z_1 = \rho + 1, \quad z_2 = \sqrt{\rho^2 - 2\rho + 2},$$
$$t = \tfrac{1}{23}(-10\rho^2 - 2\rho - 7) + \tfrac{1}{23}(-17\rho^2 + 15\rho + 18)\sqrt{\rho^2 - 2\rho + 2},$$
$$y = \tfrac{1}{23}(-13\rho^2 + 2\rho + 7) + \tfrac{1}{23}(-6\rho^2 + 8\rho + 5)\sqrt{\rho^2 - 2\rho + 2}.$$

For E_5,

$$x = \tfrac{1}{2}(\rho^2 - \rho), \quad z_1 = -\rho + 1, \quad z_2 = -\rho,$$
$$t = \tfrac{1}{23}(-5\rho^2 - \rho - 15) + \tfrac{2}{23}\sqrt{12\rho^2 - 85\rho - 56},$$
$$y = \tfrac{1}{23}(5\rho^2 + \rho - 8) + \tfrac{1}{23}(-\rho^2 + \rho + 1)\sqrt{12\rho^2 - 85\rho - 56}.$$

For E_6,

$$x = \tfrac{1}{2}(\rho^2 - 1), \quad z_1 = -\rho^2 - \rho, \quad z_2 = \rho^2 - \rho + 1,$$
$$t = \tfrac{1}{23}(-24\rho^2 + 9\rho - 3) + \tfrac{1}{23}\sqrt{-91\rho^2 - 193\rho + 72},$$
$$y = \tfrac{1}{23}(-22\rho^2 + 14\rho + 3) - \tfrac{1}{161}(3\rho^2 + 2\rho + 1)\sqrt{-91\rho^2 - 193\rho + 72}.$$

All the Humbert forms defined by these values are perfect and eutactic. Showing that these forms are eutactic according to [Coulangeon 01, Definition 2.3] amounts essentially to showing that the inverses of the matrices lie in the open convex hull of some matrix space built from the minimal vectors and the matrices themselves. Thus, having the minimal vectors and the matrices and using the inner product defined in the containing space, we found that all the eutaxy coefficients are equal to $\frac{1}{3}$; hence all the forms found are eutactic. In all, we have six perfect eutactic forms. Their gamma constants are

$$E_1 : \tfrac{4\sqrt{3}}{9} + \tfrac{2}{9}(3\rho^2 - 4\rho + 2)\sqrt{-\rho^2 + 1},$$
$$E_2 : \tfrac{4\sqrt{3}}{9} + \tfrac{2\sqrt{3}}{207}(2\rho^2 - 9\rho + 7)\sqrt{29\rho^2 + 15\rho + 41},$$
$$E_3 : \tfrac{1}{9}\left(4(\rho^2 - \rho + 1) + (4\rho^2 - 10\rho + 8)\sqrt{\rho^2 - \rho}\right) \times \sqrt{-3(\rho^2 + \rho)},$$
$$E_4 : \tfrac{2}{9}\left(-2\rho + 2 + (\rho^2 + 3\rho + 1)\sqrt{3\rho^2 - 2\rho + 2}\right) \times \sqrt{3(\rho^2 - \rho - 1)},$$
$$E_5 : \left(\tfrac{-4}{9} + \tfrac{1}{23}(\tfrac{14}{9}\rho^2 - 2\rho + 2)\sqrt{12\rho^2 - 85\rho - 56}\right) \times \sqrt{3(-\rho + 1)},$$
$$E_6 : \tfrac{2}{9}\big(2(\rho^2 - \rho + 1) + \tfrac{1}{161}(76\rho^2 - 75\rho + 50)\sqrt{-91\rho^2 - 193\rho + 72}\big) \times \sqrt{-3(\rho^2 + \rho)}.$$

We note that all these values coincide, and using the above approximation of ρ we give a numerical value for the *gamma* constant of K:

$$\gamma_{K,2} \approx 2.4684958820020039303 6032.$$

4. FINAL REMARKS

Following the work of Lenstra, [Leutbecher and Martinet 82] introduces for any number field K of degree n the constant $B(K)$, which is the lower bound of the norms of the nontrivial ideals in $\mathcal{O}_K$. It can be shown that $B(K)$ is a prime power that satisfies

$$2 \le L(K) \le B(K) \le 2^n = N_{K/\mathbb{Q}}(2\mathcal{O}_K).$$

The constant $B(K)$ gives some lower bound for $\gamma_{K,2}$ according to the following proposition.

Proposition 4.1. *Let* $[K:\mathbb{Q}] = r + 2s$. *If* $L(K) < 2r + 3s$, *then*

$$B(K) \le \gamma_{K,2}.$$

Proof: Let S be a binary Humbert form such that $\gamma(S) = \gamma_{K,2}$. In particular, S is perfect, so that $\#M(S) \ge 2r + 3s$, and we may further assume that $e_1 \in M(S)$. We claim that the condition $L(K) < 2r + 3s$ implies that there exists at least one nonunimodular minimal pair. Indeed, if this were not the case, we would have, for any $v = (\alpha, \beta)^t \in M(S)$,

$$\left| N_{K/\mathbb{Q}}\left(\det \begin{bmatrix} \alpha & 1 \\ \beta & 0 \end{bmatrix}\right)\right| = 1, \tag{4–1}$$

whence $\beta \in \mathcal{O}_K^*$. Without loss of generality we may thus assume that $v = (\alpha, 1)^t$ for all $v \in M(S)$. Then there will be a sequence of first coordinates of minimal vectors $\{\alpha_1, \alpha_2, \dots, \alpha_{2r+3s}\}$ that gives a Lenstra sequence of length $2r + 3s$. A contradiction. □

We now exhibit two fields K in which the value of the Lenstra constant and the cardinality of $\mathcal{N}_K([\gamma_{K,2}])$ allow us to follow the same computations in order to obtain the value of their binary Hermite–Humbert constants. All the fields have class number one:

$[K : \mathbb{Q}]$	defining equation	d_K	$n_K([\gamma_{K,2}])$	$L(K)$	$2r + 3s$
3	$x^3 + x^2 - x + 1$	-44	3	2	5
4	$x^4 + x^3 + x^2 + x + 1$	125	1	5	7

ACKNOWLEDGMENTS

The authors are indebted to the referee whose comments and suggestions greatly helped to improve the paper. R. Coulangeon was partially supported by Proyecto FONDECYT #7020959. M. I. Icaza was partially supported by Proyecto FONDECYT #1040670, ACT05, and by P. Reticulados y Ecuaciones Universidad de Talca, Chile. M. O'Ryan was partially supported by Proyecto FONDECYT #1040670, ACT05 and by P. Reticulados y Ecuaciones Universidad de Talca, Chile.

REFERENCES

[Baeza and Icaza 97] R. Baeza and M. I. Icaza. "On Humbert–Minkowski's Constant for a Number Field." *Proc. AMS* 125:11 (1997), 3195–3202.

[Baeza and Icaza 04] R. Baeza and M. I. Icaza. "On the Unimodularity of Minimal Vectors of Humbert Forms." *Arch. Math* 83 (2004), 528–535.

[Baeza et al. 01] R. Baeza, R. Coulangeon, M. I. Icaza, and M. O'Ryan. "Hermite's Constant for Quadratic Number Fields." *Experimental Mathematics* 10:4 (2001), 543–551.

[Borevich and Shafarevich 66] Z. I. Borevich and I. R. Shafarevich. *Number Theory.* New York: Academic Press, 1966.

[Coulangeon 01] R. Coulangeon. "Voronoi Theory over Algebraic Number Fields." *M. de L'Enseignement Mathématique, Genève* 37 (2001), 147–162.

[Icaza 97] M. I. Icaza. "Hermite Constant and Extreme Forms for Algebraic Number Fields." *J. London Math. Soc. (2)* 55 (1997), 11–22.

[Lang60] S. Lang. "Integral Points on Curves." *Inst. Hautes Études Sci. Publ. Math.* 6 (1960), 27–43.

[Lenstra 97] H. W. Lenstra Jr. "Euclidean Number Fields of Large Degree." *Invent. Math.* 38 (1997), 237–254.

[Leutbecher and Martinet 82] A. Leutbecher and J. Martinet. "Lenstra's Constant and Euclidean Number Fields." *Arithmetic Conference (Metz, 1981), Astérisque* 94 (1982), 87–131.

[Martinet 03] J. Martinet. *Perfect Lattices in Euclidean Spaces*, Grundlehren M. W., 327. Berlin: Springer, 2003.

[Nagell 64] T. Nagell. "Sur une propriété des unités d'un corps algébrique." *Ark. Mat.* 5 (1964), 343–356.

[Ohno and Watanabe 01] S. Ohno and T. Watanabe. "Estimates of Hermite Constants for Algebraic Number Fields." *Comment. Math. Univ. St. Paul* 50:1 (2001), 53–63.

[Pohst and Wagner 05] M. Pohst and M. Wagner. "On the Computation of Hermite–Humbert Constants for Real Quadratic Number Fields." *Journal de Théorie des Nombres de Bordeaux* 17 (2005), 905–920.

[Pohst and Zassenhaus 89] M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory.* New York: Cambridge University Press, 1989.

Renaud Coulangeon, Institut de Mathématiques de Bordeaux, Université Bordeaux 1, 351 Cours de la Libération, 334405 Talence, France (renaud.coulangeon@math.u-bordeaux1.fr)

Maria Inés Icaza, Instituto de Matemática y Física, Universidad de Talca, Casilla 721 Talca, Chile (icazap@inst-mat.utalca.cl)

Manuel O'Ryan, Instituto de Matemática y Física, Universidad de Talca, Casilla 721 Talca, Chile (moryan@inst-mat.utalca.cl)

Received September 7, 2006; accepted in revised form June 4, 2007.