

On the unimodularity of minimal vectors of Humbert forms

By

R. BAEZA¹⁾ and M. I. ICAZA²⁾

1. Summary. If $S = (S_1, \dots, S_m)$ is an m -tuple of $n \times n$ positive definite symmetric real matrices (= Humbert form) and K is a real number field of degree m with ring of integers \mathcal{O}_K , a vector $u \in \mathcal{O}_K^n$ is called minimal if $S[u] = \text{Min}\{S[v] \mid v \in \mathcal{O}_K^n - \{0\}\}$, where $S[v] = \prod_i S_i[v^i]$ and $v^i = i$ -th conjugate of v . In this note we show that any Humbert form S has a unimodular minimal vector over K if and only if the class number of K is 1. In [2] we introduced a constant $M_{K,n}$ which measures the non-unimodularity of minimal vectors. We estimate here the constant $M_{K,2}$ in terms of known constants of K . As a by-product we obtain a lower bound for the classical Hermite constant γ_{2m} .

2. Introduction. Let K/\mathbb{Q} be a totally real number field of degree m , with ring of integers \mathcal{O}_K and discriminant d_K . Let $h(K)$ be the class number of K and $\sigma_1, \dots, \sigma_m : K \rightarrow \mathbb{R}$ the embeddings of K into the real numbers. A Humbert form of rank n over K is an m -tuple $S = (S_1, \dots, S_m)$ of $n \times n$ positive real symmetric matrices S_1, \dots, S_m ([2]). For any matrix A with entries in K we denote by $A^{(i)}$, the i -th conjugate $\sigma_i(A)$ of A . If $u = (u_1, \dots, u_n) \in \mathcal{O}_K^n$ we define the value of S at u by $S[u] = \prod_{i=1}^m S_i[u^{(i)}]$, where $B[C]$ means CBC^t whenever this product is defined for matrices B and C . The minimum of S is defined by $m(S) = \min\{S[u] \mid 0 \neq u \in \mathcal{O}_K^n\}$, and its determinant by $\det S = \prod_{i=1}^m \det S_i$. We define the generalized Hermite constant of K by

$$\gamma_{K,n} = \sup_S m(S) / (\det(S))^{1/n}$$

Mathematics Subject Classification (2000): 11H31, 11H55.

¹⁾Partially supported by Proyecto FONDECYT 1030218, FONDECYT 1970214 and Programa de Formas Cuadráticas. Universidad de Talca, Chile.

²⁾Partially supported by Proyecto FONDECYT 1020959, FONDECYT 1990897 and Programa de Formas Cuadráticas. Universidad de Talca, Chile.

where S runs over all positive definite Humbert forms of rank n (s. [5], [2]). In particular $\gamma_{\mathbb{Q},n} = \gamma_n$ is the classical Hermite constant. A vector $u \in \mathcal{O}_K^n$ is called a minimal vector of S if $S[u] = m(S)$. In this paper we are concerned with the unimodularity of minimal vectors. Recall that a vector $u = (u_1, \dots, u_n) \in \mathcal{O}_K^n$ is unimodular if $\langle u \rangle = \mathcal{O}_K u_1 + \dots + \mathcal{O}_K u_n = \mathcal{O}_K$. If u is a minimal vector of a form S , then $\langle u \rangle$ is an ideal of minimal norm in its class. Conversely any ideal of minimal norm in its class is of this form for a suitable binary Humbert form (s. §3).

In [2] we introduced a constant $M_{K,n}$ which measures the non-unimodularity of minimal vectors (s. §3 for the definition). We show that $M_{K,n} = 1$ for all $n \geq 2$ if and only if $h(K) = 1$. As a by-product of the proof of this result one obtains a lower bound for $\gamma_{K,2}$ which is used in Section 4 to estimate from below γ_{2m} .

In Section 4 we estimate $M_{K,2}$ in terms of known invariants of the field K and in Section 6 we introduce another obstruction for the unimodularity of minimal vectors of Humbert forms.

We would like to thank the referee for simplifying the original proof of Theorem 3.1 and Corollary 3.2.

3. Unimodularity of minimal vectors. Let us recall the definition of the constant $M_{K,n}$ introduced in [2], which in some sense measures the non-unimodularity of minimal vectors of Humbert forms. For any Humbert form S over K of rank n , let $M(S)$ be the set of minimal vectors. For any $u = (u_1, \dots, u_n) \in \mathcal{O}_K^n$ we define the norm of u by

$$N(u) = \prod_{u_i \neq 0} |N_{K/\mathbb{Q}}(u_i)|$$

where $N_{K/\mathbb{Q}} : K \rightarrow \mathbb{Q}$ is the usual norm. Set

$$N(S) = \inf\{N(u) \mid u \in M(S)\}$$

and

$$N[S] = \inf\{N(S[U]) \mid U \in GL(n, \mathcal{O}_K)\},$$

where $S[U] = (S_1[U^{(1)}], \dots, S_m[U^{(m)}])$ runs over all equivalent forms to S . In [2] it is shown that $N[S]$ is bounded above by a constant depending only on K and n , so that we can define the constant

$$M_{K,n} = \sup_S N[S]$$

where S runs over all Humbert forms over K of rank n . If $h(K) = 1$ it is clear that $M_{K,n} = 1$ for all $n \geq 2$ and every form S has a unimodular minimal vector. Conversely we have

Theorem 3.1. *For any totally real number field K the following assertions are equivalent*

1. $h(K) = 1$
2. $M_{K,n} = 1$ for all $n \geq 2$

Proof. (2) follows from (1) by the definition of $M_{K,n}$. To prove the other implication it suffices to show that $M_{K,2} = 1$ implies $h(K) = 1$. Let us assume that $h(K) > 1$. Let $I \subseteq \mathcal{O}_K$ be a non-principal ideal and let $J \subseteq \mathcal{O}_K$ be an ideal in its inverse class, i.e., IJ is principal. We consider the \mathcal{O}_K -lattice $\Lambda = Ie_1 \perp Je_2 \subset K^2$ where $e_1 = (1, 0)^t$, $e_2 = (0, 1)^t$ is the standard basis and where K^2 is equipped with the standard quadratic form $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. One associates to Λ a Humbert form as follows. The lattice Λ is free since IJ is principal, so we have $\Lambda = \mathcal{O}_K e \oplus \mathcal{O}_K f$ with $e = (x_1, x_2)^t$, $f = (y_1, y_2)^t$. Then $I = \langle x_1, y_1 \rangle$, $J = \langle x_2, y_2 \rangle$. Let S be the Gram matrix of the quadratic form with respect to this basis and $S_I = (S^{(1)}, \dots, S^{(m)})$ be the associated Humbert form. Then it follows that the minimum of S_I is $m(S_I) = N(\alpha)^2$ where $\alpha \in I$ or $\alpha \in J$ is of minimal norm among all $\beta \in I \cup J$, $\beta \neq 0$ and the only minimal vectors of S_I are of the form αe_1 or αe_2 . Assume $\alpha \in I$ and set $\alpha e_1 = a_1 e + a_2 f$ with $a_1, a_2 \in \mathcal{O}_K$. Then $(a_1, a_2) \in \mathcal{O}_K^2$ is a typical minimal vector of S_I . From $\alpha = a_1 x_1 + a_2 y_1, 0 = a_1 x_2 + a_2 y_2$ it follows that (a_1, a_2) is not unimodular. This implies that S_I has no unimodular minimal vectors and hence $M_{K,2} > 1$. This proves the theorem. \square

As a by-product of the above proof one obtains a lower bound for the generalized Hermite constant $\gamma_{K,2}$ of K in the case $h(K) > 1$. Take $I \subset \mathcal{O}_K$ to be any non-principal ideal of minimal norm in its class and let $J \subset \mathcal{O}_K$ be an ideal of minimal norm in the inverse class of I . Then in the construction of the proof of the above theorem, the element α is now in I as well as in IJ . Therefore $m(S_I) = N(\alpha)^2 \geq N(I)^2 N(J)^2$ and since $\det S_I = N(\det S) = N(I)^2 N(J)^2$, we obtain

$$\gamma_{K,2} \geq \frac{m(S_I)}{(\det S_I)^{1/2}} \geq N(I)N(J) \geq 2N(I).$$

If $N(K)$ denotes the maximum of all $N(I)$ where I runs over the ideals of minimal norm in its class, we get

Corollary 3.2. *If K is a (real) number field with $h(K) > 1$, then*

$$\gamma_{K,2} \geq 2N(K).$$

For example, for $K = \mathbb{Q}(\sqrt{10})$ we know that $N(K) = 2$. Therefore $\gamma_{\mathbb{Q}(\sqrt{10}),2} \geq 4$. The constant $N(K)$ seems to be very difficult to compute. We refer to [1] for some estimates.

4. A lower bound for γ_{2m} . In this section we will use (3.2) and an idea of H. Cohn (s. [3]) to get a lower bound for the classical Hermite constant γ_{2m} . Take any (real) number field K of degree m . We assume K to be real just to simplify the notations. Let $S = (S_1, \dots, S_m)$ be a Humbert form of rank n over K . For any $u = (u_1, \dots, u_n) \in \mathcal{O}_K^n$, $u \neq 0$, we get using the arithmetic geometric inequality

$$m \left[\prod_{i=1}^m S_i[u^{(i)}] \right]^{\frac{1}{m}} \leq \sum_{i=1}^m S_i[u^{(i)}]$$

and hence

$$m [m(S)]^{\frac{1}{m}} \leq \sum_{i=1}^m S_i [u^{(i)}].$$

Let us fix a \mathbb{Z} -basis $\{w_1, \dots, w_m\}$ of \mathcal{O}_K . Then each component $u_i \in \mathcal{O}_K$ can be written $u_i = \sum_{k=1}^m x_{ik} w_k$ with $x_{ik} \in \mathbb{Z}$. Set $X = (x_{ik}) \in M_{n,m}(\mathbb{Z})$. With $w = (w_1, \dots, w_m)$ we have $u^t = Xw^t$ and hence $u = wX^t$. For each $1 \leq j \leq m$, we obtain $u^{(j)} = w^{(j)} X^t$, where $w^{(j)} = (w_1^{(j)}, \dots, w_m^{(j)})$. Then the sum $\sum_{i=1}^m S_i [u^{(i)}]$ seen as a quadratic form in the variables $\{x_{ik}\}$ is of rank mn and is given by

$$Q(X) = \sum_{i=1}^m w^{(i)} X^t S_i X w^{(i)t}.$$

Let $m(Q)$ be the minimum of $Q(X)$ taken over all $X \in M_{n,m}(\mathbb{Z})$, $X \neq 0$. We have

$$m [m(S)]^{\frac{1}{m}} \leq m(Q)$$

and therefore

$$m [m(S)]^{\frac{1}{m}} \leq \gamma_{mn} (\det Q)^{\frac{1}{mn}}$$

by the classical Hermite inequality (s. [11]). Thus we are led to compute $\det Q$. To this end we now describe the lattice Λ in \mathbb{R}^{mn} determined by the quadratic form $Q(X)$. We start with the isomorphism

$$\phi : K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \mathbb{R}^m$$

given by $\phi(a \otimes \lambda) = (\lambda \sigma_1(a), \dots, \lambda \sigma_m(a))$ where $\sigma_i : K \rightarrow \mathbb{R}$ are the embeddings of K in \mathbb{R} . We denote $K \otimes_{\mathbb{Q}} \mathbb{R}$ by \mathbb{R}_K . We have in \mathbb{R}_K the sublattice $\mathcal{O}_K \subset \mathbb{R}_K$ given by the embedding $a \mapsto a \otimes 1$. This lattice in \mathbb{R}^m has volume $|d_K|^{1/2}$. ϕ gives then an isomorphism $\mathbb{R}_K^m \rightarrow \mathbb{R}^{mn} = (\mathbb{R}^n)^m$. Write the Humbert form $S = (S_1, \dots, S_m)$ as $S = AA^t = (A_1 A_1^t, \dots, A_m A_m^t)$ with $A = (A_1, \dots, A_m) \in (GL_n(\mathbb{R}))^m$ and define $\Lambda = A\phi(\mathcal{O}_K^n) \subset \mathbb{R}^{mn}$. Then Λ is the lattice associated to Q , and Λ (and hence Q) has discriminant $\det(A)^2 |d_K|^n = \det S |d_K|^n$. Inserting this in Hermite's inequality it follows

$$m [m(S)]^{\frac{1}{m}} \leq \gamma_{mn} (\det S)^{\frac{1}{mn}} (|d_K|)^{\frac{1}{m}}$$

and this implies

$$\gamma_K(S) = \frac{m(S)}{(\det S)^{\frac{1}{n}}} \leq m^{-m} \gamma_{mn}^m |d_K|.$$

We have thus shown

Theorem 4.1. *For any (real) number field K of degree m , and for any $n \geq 1$ it holds*

$$\gamma_{K,n} \leq m^{-m} \gamma_{mn}^m |d_K|.$$

Remark 4.2. This result is essentially due to H. Cohn. In the case $h(K) = 1$ it has also been obtained using other methods by T. Watanabe (s. [9]).

Combining (4.1) with (3.2) we conclude

Corollary 4.3. *For any (real) number field K with $h(K) > 1$ and $m = [K : \mathbb{Q}]$,*

$$\gamma_{2m} \geq m \left[\frac{2N(K)}{|d_K|} \right]^{\frac{1}{m}}.$$

Remark 4.4. The special feature of the above lower bound for γ_{2m} is that it is obtained by purely arithmetical arguments. By the contrary, the well known Hlawka-Minkowski bound for γ_n , i.e.

$$\gamma_n \geq \left[\frac{2\zeta(n)}{w_n} \right]^{\frac{2}{n}}, \quad n \geq 1,$$

is obtained by analytical considerations ([11]). Let us compare both bounds for the special case $m = 2$, i.e., for γ_4 . The bound in (4.3) allows us to use any quadratic real number field with $h(K) > 1$. Take for example $K = \mathbb{Q}(\sqrt{10})$. Then $d_K = 40$ $N(K) = 2$. Thus we obtain $\gamma_4 \geq 0.63$. On the other hand the H-M bound gives $\gamma_4 \geq 0.66$. In fact we can prove that (4.3) holds true also for non real number fields.

5. An estimate of $M_{K,2}$. In this section we will estimate $M_{K,2}$ in terms of known constants of the the field K . To this end we need the following explicit description of $M_{K,2}$.

Proposition 5.1. *Let K be any (real) number field. Then*

$$M_{K,2} = \sup_I \left[\inf_{I=(\alpha,\beta)} N((\alpha, \beta)) \right]$$

where I runs over all ideals of minimal norm in its class.

Proof. We may assume $h(K) > 1$. For any binary Humbert form S over K we have $N[S] = \inf_{T \in [S]} \left(\inf_{u \in M(T)} N(u) \right)$. Hence there is some $T \in [S]$ and $u \in M(T)$ with $N[S] = N(u)$. Set $I = \langle u \rangle$. In particular I has minimal norm among the ideals in its class. If $I = \langle v \rangle$, $v \in \mathcal{O}_K^2$, there is some $U \in GL(2, \mathcal{O}_K)$ with $U[u] = v$ and hence $v \in M(T[U])$. Since $T[U] \in [S]$, we get by the choice of u , that $N(u) \leq N(v)$. In particular

$$N(u) = \inf_{\langle v \rangle = I} N(v)$$

therefore

$$N[S] \leq \sup_I [\inf_{\langle v \rangle = I} N(v)]$$

where I runs over all ideals of minimal norm in its class. Since the right hand side of this inequality does not depend on S , we obtain

$$M_{K,2} = \sup_S N[S] \leq \sup_I (\inf_{\langle v \rangle = I} N(v)).$$

Conversely let $[I]$ be any ideal class and let I_1, \dots, I_m be all ideals in $[I]$ of minimal norm. Set $n(I_i) = \inf_{\langle u \rangle = I_i} N(u)$ and choose $I_1 = I$ such that $n(I_1) \geq n(I_i)$, $1 \leq i \leq m$.

Let $I = \langle u \rangle$, $u = (\alpha, \beta) \in \mathcal{O}_K^2$ such that $n(I_1) = N(u)$. We can construct a Humbert form S with $(-\alpha, \beta) \in M(S)$ and any other vector $(x, y) \in M(S)$ satisfies $\beta x + \alpha y = 0$ (s. proof of (3.1)). It is easy to check that (x, y) has the same norm as u . For any $T \in [S]$, say $T = S[U]$, the minimal vectors of T and S correspond to each other through the transformation U , thus they generate the same ideals, and in particular they are equivalent to I . Thus by the choice of I and u we have $N[S] = N(S) = n(I)$. Hence $N[S] = \sup_{1 \leq i \leq m} [\inf_{\langle v \rangle = I_i} N(v)]$. Let us now

consider all the ideal classes $[I]_1, \dots, [I]_h$ of K and let S_i , be the corresponding Humbert forms associated to each class as before. Then we have $\sup_{1 \leq i \leq h} N[S_i] = \sup_I (\inf_{\langle v \rangle = I} N(v))$, where I runs over all ideals of minimal norm in its class. Thus we get

$$M_{K,2} = \sup_S N[S] \geq \sup_{1 \leq i \leq h} N[S_i] = \sup_I (\inf_{\langle v \rangle = I} N(v)).$$

This concludes the proof of the proposition. \square

We use now this formula to estimate $M_{K,2}$ from above. To this end let us recall the following result due to Rieger ([10]): any ideal $I \subset \mathcal{O}_K$ admits generators α, β (of any given signature) with $|N(\alpha)| < c_m |d_K| N(I)$, $|N(\beta)| < c_m^2 |d_K|^{1/2} N(I)$, where c_m is a (computable) constant depending only on $m = [K : \mathbb{Q}]$. Inserting in (5.1) the above inequalities and using Minkowski's bound for $N(I)$ (s. [8]) we obtain

Corollary 5.2. *For any number field K*

$$M_{K,2} \leq c_m^3 \frac{m!}{m^m} |d_K|^{\frac{5}{2}}.$$

Since we are only interested in the case $h(K) > 1$, one can use also the inequality (4.3) instead of Minkowski's bound, and we get

Corollary 5.3. *If $h(K) > 1$ then*

$$4N(K)^2 \leq M_{K,2} \leq c_m^3 \frac{\gamma_{2m}^{2m}}{4m^{2m}} |d_K|^{\frac{7}{2}}.$$

The inequality on the left hand side follows from (5.1) and the fact that $N(I)$ divides the norm of any element $\gamma \in I$, and since we may take I non principal in (5.1), we have $2N(I) \leq |N(\gamma)|$ for any $\gamma \in I$, $\gamma \neq 0$.

6. Another obstruction for unimodularity of minimal vectors. Let us define the proper minimum of a Humbert form S of rank n over the number field K as $m^*(S) = \min\{S[u] \mid u \in \mathcal{O}_K^n, u \text{ unimodular}\}$. Of course $m(S) \leq m^*(S)$ and there is a unimodular $u \in \mathcal{O}_K^n$ with $m^*(S) = S[u]$. We will show in this section that the number

$$U_{K,n} := \sup_S \frac{m^*(S)}{m(S)}$$

exists, where S runs over all Humbert forms of K of rank n . Hence we can define the proper Hermite constant of K , $\gamma_{K,n}^* = \sup_S \frac{m^*(S)}{(\det S)^{1/n}}$ and we obtain $\gamma_{K,n} \leq \gamma_{K,n}^* \leq U_{K,n} \gamma_{K,n}$. All this follows from

Theorem 6.1. *Let K/\mathbb{Q} be a (real) number field. Then for any Humbert form S over K of rank n there exists a unimodular vector $u \in \mathcal{O}_K^n$ with*

$$S[u] \leq u_{K,n} m(S),$$

where $u_{K,n}$ is a constant depending only on K and n .

Proof. For any $n \times n$ matrix $A \in M_n(K)$ with $\det A \neq 0$, set $\|A\| = \max\{\|A^{(i)}\|, 1 \leq i \leq m\}$ and $l(A) = \min\{l(A^{(i)}), 1 \leq i \leq m\}$, where for any real $B \in GL(n, \mathbb{R}), \|B\|$ denotes the usual norm and $l(B) = \|B^{-1}\|^{-1}$ (s.[L-T]). Since S is a Humbert form there is some $B = (B_1, \dots, B_m) \in GL(n, \mathbb{R})^m$ such that $S = BB^t = (B_1 B_1^t, \dots, B_m B_m^t)$. Then for any $x \in K^n$ $S[x] = \prod_{i=1}^m \|x^{(i)} B_i\|^2$ and $S[A][x] = \prod_{i=1}^m \|x^{(i)} A^{(i)} B_i\|^2$. Using standard norm estimates we obtain $l(A)^{2m} S[x] \leq S[A][x] \leq \|A\|^{2m} S[x]$. Therefore

$$l(A)^{2m} m(S) \leq m(S[A]) \leq \|A\|^{2m} m(S).$$

We now use Humbert’s reduction theory (s. [4]). It states that for any Humbert form S there is a $U \in GL(n, U)$ with $S[U] \in R_{K,n}$, where $R_{K,n}$ is the cone of Humbert reduced forms. Moreover there exists a finite set $\{A_1, \dots, A_t\}$ of non-singular $n \times n$ -matrices over K , depending only on K and n , such that for any $R \in R_{K,n}$ there is $1 \leq i \leq t$ such that $e = (1, \dots, 0)$ is a minimal vector of $R[A_i]$. Thus, let us take $U \in GL(n, \mathcal{O}_K)$ with $S_0 = S[U] \in R_{K,n}$ and let $1 \leq i \leq n$ be such that e is a minimal vector of $S_0[A_i]$. Let $A = A_i$. Then $m(S_0[A]) = S_0[A][e]$ and hence $\|A\|^{2m} m(S) \geq S_0[A][e]$. Let $a_{K,n} = \max\{\|A_i\|^{2m}, 1 \leq i \leq t\}$ and $b_{K,n} = \inf\{\ell(A_i)^{2m}, 1 \leq i \leq t\}$ constants depending only on K and n . We get

$$a_{K,n} m(S) \geq S_0[A][e] = \prod_{i=1}^m S_{oi}[A^{(i)}][e] \geq \prod_{i=1}^m l(A^{(i)})^2 S_{oi}[e] \geq b_{K,n} S_0[e].$$

From $S_0 = S[U]$ we obtain $S_0[e] = S[u]$ with $u = Ue \in \mathcal{O}_K^n$ unimodular. Thus we have $a_{K,n} m(S) \geq b_{K,n} S[u]$ and this proves the claim with $u_{K,n} = a_{K,n} b_{K,n}^{-1}$. \square

It would be interesting to compare both constants $M_{K,n}$ and $U_{K,n}$. We do not know of any estimate of $U_{K,n}$.

References

- [1] E. A. ANFER'EVA and N. G. CHUDAKOV, Effective estimates from below of the norm of ideals of an imaginary quadratic field. *Mat. USSR Sb.* **11**, no 1, 47–58 (1970).
- [2] R. BAEZA and M. I. ICAZA, On Humbert-Minkowski's constant for a number field. *Proc. Amer. Math. Soc.* **125**, 3195–3202 (1997).
- [3] H. COHN, On the shape of the fundamental domain of the Hilbert modular group. *Theory of numbers.* A. L. Whiteman, ed., *Proc. Symp. Pure Math.* **8**, 190–202 (1965).
- [4] P. HUMBERT, Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique K fini. *Comm. Math. Helv.* **12**, 263–306 (1940).
- [5] M. I. ICAZA, Hermite constant and extreme forms for algebraic number fields. *J. London Math. Soc.* **55**, 11–22 (1997).
- [6] P. LANCASTER and M. TISMENETSKY, *The theory of matrices*, 2nd. Ed. 1985.
- [7] J. MARTINET, Perfect lattices in Euclidean spaces. *Grundlehren Math. Wiss.* **327**, 2003.
- [8] W. NARKIEWICZ, *Elementary and analytic theory of algebraic numbers*, 2nd. Ed. 1990.
- [9] S. OHNO and T. WATANABE, Estimates of Hermite constants for algebraic number fields. *Comm. Math. Univ. St. Paul.* **50** (1), 53–63 (2001).
- [10] G. J. RIEGER, Einige Sätze über Ideale in algebraischen Zahlkörpern. *Math. Ann.* **136**, 339–341 (1958).
- [11] C. L. SIEGEL, *Lectures on the geometry of numbers*. 1989.

Received: 28 November 2003; revised manuscript accepted: 13 April 2004

R. Baeza and M. I. Icaza
Instituto de Matemáticas
Universidad de Talca
Casilla 721
Talca
Chile
rbaeza@inst-mat.otalca.cl
icazap@inst-mat.otalca.cl