Proc. Estonian Acad. Sci. Phys. Math., 2005, **54**, 4, 195–211
https://doi.org/10.3176/phys.math.2005.4.01

On additive generalization of Voronoï's theory to algebraic number fields

Alar Leibak

Department of Mathematics, Faculty of Science, Tallinn University of Technology, Ehitajate tee 5, 19086 Tallinn, Estonia; aleibak@edu.ttu.ee

Received 12 April 2004, in revised form 28 June 2005

Abstract. A generalization of Voronoï's theory to perfect quadratic form over algebraic number fields is studied. This generalization follows Koecher's idea (see *Math. Ann.*, 1960, **141**, 384–432) of using the minimums of $\mathrm{Tr} f(X)$ for the positive definite quadratic form $f(X)$. As a result some useful properties of perfect quadratic forms are presented and the upper and lower bounds of Hermite's constant are proved.

Key words: perfect quadratic forms, algebraic number fields.

1. INTRODUCTION

In this paper an additive generalization of Voronoï's theory to algebraic number fields is studied. Using *trace minimums* (i.e. minimums of quadratic form $\mathrm{Tr} f(X)$; see Eq. (1)) it is possible to introduce perfect forms, extreme forms, and the generalization of Hermite's constant. Koecher [1] introduced the perfect forms with respect to the trace minimums and, following his work, Ong [2,3] studied binary perfect forms over real quadratic fields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{5})$. It should be pointed out that the systematic approach to this generalization has not been published so far.

The present paper was motivated also by the difference between this generalization (herein called *additive* generalization) and *multiplicative* generalization introduced in Baeza and Icaza [4] and Icaza [5] (they consider *norm minimums* i.e. minimums of $\mathrm{Nm} f(X)$) and completed in Coulangeon [6]. Let us consider the following example. Let $\mathbb{K}$ be a totally real algebraic number field and let $a \in \mathbb{K}$ be totally positive. We write $\mathcal{O}_{\mathbb{K}}$ for the ring of algebraic integers of $\mathbb{K}$. The function $\gamma^*_{\mathbb{K}}$ is defined for unary forms by the equation

$$\gamma^*_{\mathbb{K}}(ax^2) = \frac{\min\{\mathrm{Nm}_{\mathbb{K}/\mathbb{Q}}(ax^2) | x \in \mathcal{O}_{\mathbb{K}} \setminus \{0\}\}}{\mathrm{Nm}_{\mathbb{K}/\mathbb{Q}}(a)}$$

(see [5], Remark 1, p. 12). As $\mathrm{Nm}_{\mathbb{K}/\mathbb{Q}}(x^2) \geq 1$ for all $x \in \mathcal{O}_{\mathbb{K}}$, and the equality $\mathrm{Nm}_{\mathbb{K}/\mathbb{Q}}(x^2) = 1$ holds at units of $\mathcal{O}_{\mathbb{K}}$, we have $\gamma^*_{\mathbb{K}}(ax^2) = 1$ for each totally positive $a \in \mathbb{K}$. In multiplicative generalization, Coulangeon considered Humbert tuples up to scaling (see [6]). Consequently, from the multiplicative point of view, there is only one unary form which is of course extreme. Hence, the situation in dimension one is trivial from the multiplicative point of view. For additive generalization, let us consider the number field $\mathbb{Q}(\sqrt{3})$. Let $e > 1$ denote the fundamental unit in $\mathbb{Q}(\sqrt{3})$. In our case Hermite's function $\gamma_{\mathbb{Q}(\sqrt{3})}$ on a positive definite unary form ax^2 is defined by

$$\gamma_{\mathbb{Q}(\sqrt{3})}(ax^2) = \frac{\min\{\mathrm{Tr}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(ax^2) | x \in \mathcal{O}_{\mathbb{Q}(\sqrt{3})} \setminus \{0\}\}}{\sqrt{\mathrm{Nm}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(a)}}.$$

An immediate computation shows that

$$\gamma_{\mathbb{Q}(\sqrt{3})}(ex^2) = 4 > \gamma_{\mathbb{Q}(\sqrt{3})}(ax^2)$$

for any unary form ax^2 that is neither equivalent nor homothetic to the unary form ex^2. Hence, ex^2 is a critical unary form over $\mathbb{Q}(\sqrt{3})$ (see Definition 4). See also Example 1 for the difference of perfect forms in these generalizations.

Perfect forms (in the sense of additive generalization) are closely related to the reduction theory of positive definite quadratic forms over algebraic number fields (see [1,7]). The explicit descriptions of these reduction domains have not been published by now, which also motivates the study of additive generalization.

As a result, the necessary conditions of the well-known Voronoï's theorem are generalized to algebraic number fields (Theorem 5).

Given a unary perfect form over a totally real algebraic number field $\mathbb{K}$, a method for obtaining an initial perfect quadratic form of rank m over $\mathbb{K}$ is presented (Theorem 1 and Remark 2). Ong (see Theorem 3.2.1 in [3]) gave a construction of initial perfect forms for number fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{5})$. Ong's result will be generalized to an arbitrary totally real algebraic number field (Theorems 1 and 2). Once we have an initial perfect form of rank m over $\mathbb{K}$, we can find all perfect forms (up to equivalence) of rank m over $\mathbb{K}$ by applying Voronoï's algorithm. Among these perfect forms there is a quadratic form $a\phi_0^{(m)}$ such that the unary form ax^2 is perfect over $\mathbb{K}$ and $\phi_0^{(m)}$ is the principal perfect form over $\mathbb{Q}$ of rank m

$$\phi_0^{(m)}(x_1, \ldots, x_m) = \sum_{i=1}^{m} x_i^2 + \sum_{i=1}^{m} \sum_{j=i+1}^{m} x_i x_j.$$

Hence, by Theorem 1 and by applying the generalization of Voronoï's algorithm (to binary quadratic forms over real quadratic fields, see [2,3]) it is possible to find all perfect quadratic forms (up to equivalence and homothety) over $\mathbb{K}$.

Section 4 is concluded with the upper bound of the additive Hermite's constant in terms of the number field and the rational Hermite's constant (Theorem 6). It is shown that the given upper bound is the best possible. In Section 5 it is indicated how these results can be used to show that particular binary forms are critical. In these examples new constructions for lattices E_6 and E_8 are presented.

2. DEFINITIONS AND NOTATIONS

Let $\mathbb{K}$ be an algebraic number field with r real embeddings $\sigma_1, \dots, \sigma_r$ and $2s$ complex embeddings $\sigma_{r+1}, \dots, \sigma_{r+2s}$, with $\sigma_{r+s+i} = \bar{\sigma}_{r+i}$ for $1 \leq i \leq s$, where the overbar " $^-$ " denotes the complex conjugate.

Definition 1. *A tuple $(f_i)_{i=1}^{r+s}$ of r positive definite quadratic forms $f_1, \dots, f_r$ of rank m and s positive definite Hermitian forms $f_{r+1}, \dots, f_{r+s}$ of rank m is called a Humbert tuple of rank m.*

For each Humbert tuple $(f_i)_{i=1}^{r+s}$ we associate a tuple of r symmetric and s Hermitian matrices $(A_i)_{i=1}^{r+s}$ such that $f_i(x) = \bar{x}^t A_{\sigma_i} x$ for all $1 \leq i \leq r+s$.

A quadratic form (Hermitian form) f over a totally real number field (respectively a totally complex number field) $\mathbb{K}$ is said to be positive definite if $\sigma_i(f)$ is positive definite for each $i = 1, \dots, r$ (respectively $i = 1, \dots, s$).

Let $\tau_i \colon \sigma_1(\mathbb{K}) \to \sigma_i(\mathbb{K})$, $i = 2, \dots, r$, and $\tau'_j \colon \sigma_{r+1}(\mathbb{K}) \to \sigma_j(\mathbb{K})$, $j = r+2, \dots, r+s$, be field isomorphisms.

Definition 2. *A Humbert tuple $(f_1, \dots, f_{r+s})$ is called a conjugate tuple if there exist a positive definite quadratic form f over $\sigma_1(\mathbb{K})$ and a Hermitian form h over $\sigma_{r+1}(\mathbb{K})$ such that*

$$(f_1, \dots, f_{r+s}) = (f, \tau_2(f), \dots, \tau_r(f), g, \tau'_{r+2}(g), \dots, \tau'_{r+s}(g)).$$

If $\mathbb{K}$ is totally real (totally complex), then a Humbert tuple $(f_1, \dots, f_r)$ (respectively $(f_1, \dots, f_s)$) is called a conjugate tuple if there exist a positive definite quadratic form over $\mathbb{K}$ (respectively a positive definite Hermitian form h over $\mathbb{K}$) such that $(f_1, \dots, f_r) = (\sigma_1(f), \dots, \sigma_r(f))$ (respectively $(f_1, \dots, f_s) = (\sigma_1(h), \dots, \sigma_s(h))$).

If $\mathbb{K}$ is totally real (totally complex) and f is a positive definite quadratic form (respectively a positive definite Hermitian form) over $\mathbb{K}$, then we use the same letter f for the Humbert tuple $(\sigma_1(f), \dots, \sigma_r(f))$ (respectively $(\sigma_1(f), \dots, \sigma_s(f))$).

Throughout this paper, $\mathcal{P}_{m,\mathbb{K}}$ denotes the set of all Humbert tuples of rank m over a number field $\mathbb{K}$.

The group $\mathrm{GL}(m, \mathbb{K})$ acts on $\mathcal{P}_{m,\mathbb{K}}$ via the embedding

$$\mathrm{GL}(m, \mathbb{K}) \hookrightarrow \mathrm{GL}(m, \mathbb{R})^r \times \mathrm{GL}(m, \mathbb{C})^s, \qquad M \rightsquigarrow (\sigma_i(M))_{i=1}^{r+s}.$$

By the trace minimum of the Humbert tuple $(f_1, \ldots, f_{r+s})$ of rank m we mean the set $\mathcal{M}(f)$ of nonzero vectors $X \in \mathcal{O}_{\mathbb{K}}^m$ where the positive definite quadratic form (over $\mathbb{R}$)

$$\sum_{i=1}^{r} f_i(\sigma_i(X)) + 2 \sum_{i=r+1}^{r+s} f_i(\sigma_i(X)) \tag{1}$$

of $m \cdot [\mathbb{K} \colon \mathbb{Q}]$ variables attains its first minimum λ_1 (i.e. the smallest nonzero value on $\mathbb{Z}^{m\cdot[\mathbb{K}\colon \mathbb{Q}]}$). If f is either a positive definite quadratic form over totally real $\mathbb{K}$ or a positive definite Hermitian form over totally complex $\mathbb{K}$, then the quadratic form (1) over $\mathbb{R}$ is $\mathrm{Tr} f(X)$. (This explains the name *trace minimum*.) If f is a Humbert tuple, then we write $\mathrm{Tr} f(X)$ for the quadratic form (1). Obviously, $\mathrm{Tr} f(X)$ is positive definite if f_i is positive definite for all $i = 1, \ldots, r + s$.

Definition 3. *A Humbert tuple $(f_i)_{i=1}^{r+s}$ is perfect if it is uniquely determined by its trace minimums and λ_1.*

By definition, a Humbert tuple f of rank m has

$$N = r\frac{m(m+1)}{2} + sm^2$$

coefficients. Hence, if f is also perfect, then we must have $\#\mathcal{M}(f) \geq N$ (for quadratic forms over real numbers see also [8]).

Let us consider a function on Humbert tuples of rank m

$$\gamma_{\mathbb{K}}(f) = \frac{\min\{\mathrm{Tr} f(X) \,|\, 0 \neq X \in \mathcal{O}_{\mathbb{K}}^m\}}{d(f)^{1/m\cdot[\mathbb{K}\colon \mathbb{Q}]}},$$

where

$$d(f) = \prod_{i=1}^{r} \det(f_{\sigma_i}) \cdot \prod_{i=r+1}^{r+s} \det(f_i)^2.$$

The real number $d(f)$ is called the determinant of the Humbert tuple f.

Clearly, $\gamma_{\mathbb{K}}(f)$ is invariant under the action by $\mathrm{GL}(m, \mathcal{O}_{\mathbb{K}})$ and multiplication by positive real scalars.

Definition 4. *A Humbert tuple f of rank m is called extreme* (*critical*) *if the function $\gamma_{\mathbb{K}}$ attains a local maximum* (*respectively a global maximum*) *at f.*

The *additive Hermite's constant* $\gamma_{m,\,\mathbb{K}}$ is defined by

$$\gamma_{m,\,\mathbb{K}} = \sup_{f \in \mathcal{P}_{m,\,\mathbb{K}}} \gamma_{\mathbb{K}}(f).$$

Definition 5. *The Humbert tuple f with the corresponding tuple of matrices $(A_i)_{i=1}^{r+s}$ is called weakly eutactic if the adjoint matrix $\widetilde{A_i}$ lies in the open convex hull of $\sigma_i(X\overline{X}^t)$, $X \in \mathcal{M}(f)$, for all $1 \le i \le r+s$, that is, there exist $(r+s)$-tuples of positive reals $\rho^X \in (\mathbb{R}_{>0})^{r+s}$, $X \in \mathcal{M}(f)$ such that*

$$\widetilde{A_i} = \sum_{X \in \mathcal{M}(f)} \rho_i^X \sigma_i(X\overline{X}^t),$$

holds for all $1 \le i \le r+s$.

The name "weak eutaxy" is due to Coulangeon (see [6]). Icaza [5] called such Humbert tuples eutactic forms. For quadratic forms over real numbers this definition coincides with the usual definition of eutaxy (see [8,9]).

3. PERFECT QUADRATIC FORM

For the convenience of the readers, we recall here the definition of a perfect Humbert tuple from [1].

Proposition 1. *Let f be a Humbert tuple of rank m with the corresponding tuple of matrices $(A_i)_{i=1}^{i=r+s}$. Then f is perfect if and only if there exist*

$$N = r\frac{m(m+1)}{2} + sm^2$$

trace minimum vectors $X_1, \ldots, X_N \in \mathcal{M}(f)$ such that the block-diagonal matrices

$$\operatorname{diag}\{\sigma_1(X_i\overline{X_i}^t), \ldots, \sigma_{r+s}(X_i\overline{X_i}^t)\}, \qquad i = 1, \ldots, N,$$

are linearly independent.

Remark 1. This was the definition for perfection given by Koecher (see [1]).

The proof is obvious (see also [2], pp. 15–16; [3]; [9], Theorem 3.2.10).

Proposition 2. *Let f be a Humbert tuple over $\mathbb{K}$. Assume that $\lambda_1 \in \mathbb{R}_{>0}$ is the trace minimum of f. If f is perfect, then there exist a conjugate tuple h over $\mathbb{K}$ and $a \in \mathbb{R}_{>0}$ such that $f = ah$.*

Proof. Let $\mathbb{K} = \mathbb{Q}(\xi)$ for some algebraic number ξ. Let $V_1, \ldots, V_T$ be the trace minimum vectors of $f = (f_1, \ldots, f_{r+s})$. By assumption, $\mathrm{Tr} f(V_l) = \lambda_1$ for all $1 \le l \le T$. Let $h = \frac{1}{\lambda_1} f$. Obviously h is a perfect Humbert tuple with minimum vectors $V_1, \ldots, V_T$ and $\mathrm{Tr}\, h(V_i) = 1$ for all $1 \le i \le T$. It remains to prove that h is a conjugate tuple. By Definition 3, the system of linear equations

$$\mathrm{Tr}\, h(V_k) = 1, \quad k = 1, \ldots, T, \tag{2}$$

yields the unique solution (the Humbert tuple h). After expanding the system (2) we have

$$\sum_{l=1}^{r}\sum_{i=1}^{m} h_{l,ii}\sigma_l(V_{k,i}^2)+2\sum_{l=1}^{r}\sum_{i=1}^{m}\sum_{j>i}^{m} h_{l,ij}\sigma_l(V_{k,i}V_{k,j})+2\sum_{l=r+1}^{r+s}\sum_{i=1}^{m} h_{l,ii}\sigma_l(V_{k,i}\overline{V_{k,i}})$$
$$+4\sum_{l=r+1}^{r+s}\sum_{i=1}^{m}\sum_{j>i}^{m}\left[\Re(h_{l,ij})\Re(\sigma_l(V_{k,i}\overline{V_{k,j}}))-\Im(h_{l,ij})\Im(\sigma_l(V_{k,i}\overline{V_{k,j}}))\right]=1,$$

where $1 \leq k \leq T$ (here $\Re$ and $\Im$ denote the real and imaginary parts, respectively). Applying Cramer's formula to the linearly independent subsystem of system (2), we get $h_{k,ij}$ as the expression of determinants. Since any algebraic number $\alpha \in \mathbb{K}$ is a $\mathbb{Q}$-linear combination of $1, \xi, ..., \xi^{[\mathbb{K}:\mathbb{Q}]-1}$, we obtain $\sigma_l(\alpha)$ from $\sigma_k(\alpha)$ by exchanging $k \leftrightarrow l$. Hence, exchanging $k \leftrightarrow l$ (i.e. $\sigma_k(\xi) \leftrightarrow \sigma_l(\xi)$) in the expression of $h_{k,ij}$, we get $h_{l,ij}$. Clearly, $h_{k,ij} \in \sigma_k(\mathbb{K})$ for any i and j.

The proposition is proved. □

Corollary 1. *If* $(a_1x^2, \ldots, a_rx^2)$ *is a perfect unary Humbert tuple over a totally real number field* $\mathbb{K}$*, then* $(a_1, \ldots, a_r) = (\sigma_1(a), \ldots, \sigma_r(a))$ *for a totally positive algebraic number* $a \in \mathbb{K}$.

For the rest of the paper, we identify unary perfect Humbert tuples $(\sigma_i(a)x^2)_{i=1}^r$ with ax^2 for some totally positive $a \in \mathbb{K}$. (This involves no loss of generality.)

Corollary 2. *Any perfect Humbert tuple over a totally real* (*totally complex*) *number field* $\mathbb{K}$ *is proportional to a positive definite quadratic* (*respectively positive definite Hermitian*) *form* f *over* $\mathbb{K}$.

Coulangeon [6] proved that any multiplicatively perfect Humbert tuple over $\mathbb{K}$ is equivalent (once conveniently rescaled) to the Humbert tuple with entries in finite extension $\mathbb{L}$ of $\mathbb{K}$. Baeza et al. [10] found that the multiplicatively extreme binary quadratic Humbert form over $\mathbb{Q}(\sqrt{2})$, which is also a multiplicatively perfect Humbert tuple, has entries in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Let us consider an example to illustrate the difference between additive generalization and multiplicative generalization.

Example 1. From the multiplicative point of view, there exists only one class of multiplicatively perfect binary forms over $\mathbb{Q}(\sqrt{D})$ for each $D = 2, 3, 5$ (see [10]). Ong [3] proved that there are at least two classes of perfect forms over $\mathbb{Q}(\sqrt{D})$ for each $D = 2, 3, 5$. For the convenience of the reader we present here the list of binary perfect forms over $\mathbb{Q}(\sqrt{D})$, $D = 2, 3, 5$, and the list of multiplicatively perfect binary forms over the same fields. Let $e > 1$ denote the fundamental unit in $\mathbb{Q}(\sqrt{D})$, $D = 2, 3, 5$. Write $\bar{e}$ for the field conjugate of e.

D	Binary perfect forms over $\mathbb{Q}(\sqrt{D})$	Multiplicatively perfect binary forms over $\mathbb{Q}(\sqrt{D})$
2	$\left(\begin{pmatrix} e\sqrt{2} & \frac{e\sqrt{2}}{2} \\ \frac{e\sqrt{2}}{2} & e\sqrt{2} \end{pmatrix}, \begin{pmatrix} -\bar{e}\sqrt{2} & \frac{-\bar{e}\sqrt{2}}{2} \\ \frac{-\bar{e}\sqrt{2}}{2} & -\bar{e}\sqrt{2} \end{pmatrix}\right),$ $\left(\begin{pmatrix} e\sqrt{2} & e \\ e & e\sqrt{2} \end{pmatrix}, \begin{pmatrix} -\bar{e}\sqrt{2} & \bar{e} \\ \bar{e} & -\bar{e}\sqrt{2} \end{pmatrix}\right)$	$\left(\begin{pmatrix} 1 & e/2 \\ e/2 & \frac{\sqrt{6}+\sqrt{2}}{2} \end{pmatrix}, \begin{pmatrix} 1 & \bar{e}/2 \\ \bar{e}/2 & \frac{\sqrt{6}-\sqrt{2}}{2} \end{pmatrix}\right)$
3	$\left(\begin{pmatrix} e & e/2 \\ e/2 & e \end{pmatrix}, \begin{pmatrix} \bar{e} & \bar{e}/2 \\ \bar{e}/2 & \bar{e} \end{pmatrix}\right),$ $\left(\begin{pmatrix} e & 2e\sqrt{3}/3 \\ 2e\sqrt{3}/3 & e \end{pmatrix}, \begin{pmatrix} \bar{e} & -2\bar{e}\sqrt{3}/3 \\ -2\bar{e}\sqrt{3}/3 & \bar{e} \end{pmatrix}\right),$ $\left(\begin{pmatrix} 2+\frac{2}{3}\sqrt{3} & 1+\sqrt{3} \\ 1+\sqrt{3} & 2+\frac{2}{3}\sqrt{3} \end{pmatrix}, \begin{pmatrix} 2-\frac{2}{3}\sqrt{3} & 1-\sqrt{3} \\ 1-\sqrt{3} & 2-\frac{2}{3}\sqrt{3} \end{pmatrix}\right)$	$\left(\begin{pmatrix} 1 & e/2 \\ e/2 & e \end{pmatrix}, \begin{pmatrix} 1 & \bar{e}/2 \\ \bar{e}/2 & \bar{e} \end{pmatrix}\right)$
5	$\left(\begin{pmatrix} e\sqrt{5} & e\sqrt{5}/2 \\ e\sqrt{5}/2 & e\sqrt{5} \end{pmatrix}, \begin{pmatrix} -\bar{e}\sqrt{5} & -\bar{e}\sqrt{5}/2 \\ -\bar{e}\sqrt{5}/2 & -\bar{e}\sqrt{5} \end{pmatrix}\right),$ $\left(\begin{pmatrix} e\sqrt{5} & e^2\sqrt{5}/2 \\ e^2\sqrt{5}/2 & e\sqrt{5} \end{pmatrix}, \begin{pmatrix} -\bar{e}\sqrt{5} & -\bar{e}^2\sqrt{5}/2 \\ -\bar{e}^2\sqrt{5}/2 & -\bar{e}\sqrt{5} \end{pmatrix}\right)$	$\left(\begin{pmatrix} 1 & -e/2 \\ -e/2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -\bar{e}/2 \\ -\bar{e}/2 & 1 \end{pmatrix}\right)$

(This example was pointed out by an anonymous referee.)

By a positive lattice we mean the lattice associated to a positive definite quadratic form. Recall that a positive lattice L (over $\mathbb{Z}$) is of *E*-type if for any positive lattice L' the minimum vectors of $L \otimes L'$ can be written as $l \otimes l'$, where $l \in L$ and $l' \in L'$ (see [11], §7.1). We refer to [11] for more facts and the existence of positive lattices of *E*-type.

Proposition 3. *Let $f(x) = \sum f_{ij}x_ix_j$ be a perfect quadratic form over $\mathbb{Z}$ and L be the corresponding lattice. If L is of E-type, then the Humbert tuple $(f, \ldots, f)([\mathbb{K}\colon \mathbb{Q}]$ copies) is not perfect over any algebraic number field $\mathbb{K}$.*

Proof. Throughout this proof m denotes the rank of f. Write $n = [\mathbb{K}\colon \mathbb{Q}]$. Let L_1 denote the lattice of the rational quadratic form $\mathrm{Tr}(x^2)$. Since L is of *E*-type, we have that minimal vectors of $L_1 \otimes L$ can be written as $l_1 \otimes l$, where l_1 is a minimum vector of $\mathrm{Tr}(x^2)$ and l is a minimum vector of f. Write $\min(f) = \{f(l) | l \in \mathbb{Z}^m \setminus \{0\}\}$. Clearly, the first minimum of the Humbert tuple $(f, \ldots, f)$ is $n \cdot \min(f)$. Applying the inequality between arithmetic and geometric means, we have

$$\mathrm{Tr}(v^2) \geq n\sqrt[n]{\mathrm{Nm}(v^2)} \geq n.$$

The first equality holds iff v^2 is an integer and the second equality holds iff v^2 is a unit in $\mathcal{O}_{\mathbb{K}}$. Combining these equalities, we obtain $v \in \mathbb{Z}$. Hence, there are only $m(m+1)/2$ linearly independent block-diagonal matrices (see Definition 1). This proves that the Humbert tuple $(f, \ldots, f)$ is not perfect. □

Nevertheless, we have a method to obtain perfect forms over a totally real number field $\mathbb{K}$ from perfect quadratic forms over $\mathbb{Q}$.

Theorem 1. *Let $\mathbb{K}$ be a totally real algebraic number field and let $\mathcal{O}_{\mathbb{K}}$ denote its ring of integers. Let ax^2 be a perfect unary quadratic form over $\mathcal{O}_{\mathbb{K}}$ with lattice L_a over $\mathbb{Z}$ and let g be a perfect quadratic form over $\mathbb{Z}$ with lattice L. If L_a or L is of E-type, then the quadratic form ag is perfect over $\mathbb{K}$.*

Proof. Let $m = \operatorname{rank}(g)$. Let $v_1, \dots, v_t \in \mathcal{O}_{\mathbb{K}}$ be the trace minimum vectors of the unary form ax^2 and let $V_1, \dots, V_T \in \mathbb{Z}^m$ be the minimum vectors of g. Hence, by the hypothesis (L_a or L is of E-type), the trace minimum vectors of ag are $v_i V_j$ ($1 \le i \le t$ and $1 \le j \le T$), and so $\lambda_1 = \operatorname{Tr}(ag(v_i V_j))$ is a rational number. Seeking a contradiction, suppose there exists a Humbert tuple $(h_1, \dots, h_r)$ of rank m over $\mathbb{K}$ such that $\operatorname{Tr}(h(v_i V_j)) = \lambda_1$ for all $1 \le i \le t$ and $1 \le j \le T$. For $1 \le p \le t$ and $1 \le q \le T$ we have

$$\begin{aligned}
\lambda_1 &= \sum_{l=1}^{r} \left(\sum_{i=1}^{m} h_{l,\,ii}\sigma_l(v_p^2)V_{q,\,i}^2 + 2\sum_{i=1}^{m}\sum_{j>i}^{m} h_{l,ij}\sigma_l(v_p^2)V_{q,i}V_{q,j} \right) \\
&= \sum_{i=1}^{m} \left(\sum_{l=1}^{r} h_{l,ii}\sigma_l(v_p^2) \right) V_{q,\,i}^2 + 2\sum_{i=1}^{m}\sum_{j>i}^{m} \left(\sum_{l=1}^{r} h_{l,ij}\sigma_l(v_p^2) \right) V_{q,i}V_{q,j}.
\end{aligned}$$

Since $V_1, \dots, V_T$ determine the quadratic form g up to positive scalar multiple, we get

$$c \cdot g_{ij} = \sum_{l=1}^{r} h_{l,ij}\sigma_l(v_p^2), \qquad 1 \le p \le t.$$

Fixing i and j, by the perfection of ax^2 we have

$$(h_{1,ij}, \dots, h_{n,ij}) = H_{ij}(\sigma_1(a), \dots, \sigma_r(a)), \qquad H_{ij} \in \mathbb{Q}.$$

This gives us the rational quadratic form

$$H(x_1, \dots, x_m) = \sum_{i=1}^{m} H_{ii}x_i^2 + 2\sum_{i=1}^{m}\sum_{j>i} H_{ij}x_i x_j.$$

Finding the trace values of ag and aH at vV for any $v \in \mathcal{M}(ax^2)$ and $V \in \mathcal{M}(g)$, we obtain

$$\operatorname{Tr}(av^2)g(V) = \lambda_1 = \operatorname{Tr}(av^2)H(V).$$

Therefore $g = H$ and ag is uniquely determined by its trace minimum vectors. The theorem is proved. □

Let $e > 1$ be the fundamental unit of a real quadratic number field $\mathbb{Q}(\sqrt{D})$. If a quadratic form f is over a number field $\mathbb{K}$, then we denote it briefly by $f/\mathbb{K}$. We can immediately verify that the unary forms $e\sqrt{2}x^2/\mathbb{Q}(\sqrt{2})$, $ex^2/\mathbb{Q}(\sqrt{3})$, and $e\sqrt{5}x^2/\mathbb{Q}(\sqrt{5})$ are perfect. Hence, this theorem generalizes the theorem proved by Ong (Theorem 3.2.1 in [3]).

Theorem 2. *Let $\mathbb{K}_1$ and $\mathbb{K}_2$ be totally real number fields with degree r_1 and r_2, respectively. Let f_1 and f_2 be perfect quadratic forms over $\mathbb{K}_1$ and $\mathbb{K}_2$, respectively. Denote the rank of f_i by m_i $(i = 1, 2)$. We define $\mathcal{L}_2(\mathcal{M}(f))$ to be the $\mathbb{Q}$-linear space generated by $\{uu^t | u \in \mathcal{M}(f)\}$. If*
1. *$\mathbb{K}_1$ and $\mathbb{K}_2$ are linearly disjoint*[1] *and* $\gcd(\mathrm{disc}(\mathbb{K}_1), \mathrm{disc}(\mathbb{K}_2)) = 1$;
2. $\{v \otimes w \,|\, v \in \mathcal{M}(f_1), w \in \mathcal{M}(f_2)\} \subseteq \mathcal{M}(f_1 \otimes f_2)$;
3. $\dim \mathcal{L}_2(\mathcal{M}(f_1)) \cdot \dim \mathcal{L}_2(\mathcal{M}(f_2)) \geqslant r_1 r_2 \frac{m_1 m_2 (m_1 m_2 + 1)}{2}$,
then $f_1 \otimes f_2$ is a perfect quadratic form over $\mathbb{K}_1\mathbb{K}_2$.

Proof. Since the number fields $\mathbb{K}_1$ and $\mathbb{K}_2$ are linearly disjoint and their discriminants are mutually prime, it follows that the ring $\mathcal{O}_{\mathbb{K}_1\mathbb{K}_2}$ is generated by $o_1 \otimes o_2 = o_1 o_2$, where $o_1 \in \mathcal{O}_{\mathbb{K}_1}$ and $o_2 \in \mathcal{O}_{\mathbb{K}_2}$ (see Ch. 3 in [12]). The rank of $f_1 \otimes f_2$ is $m_1 m_2$.

Write $r = r_1 r_2$. Let $\sigma_1, \ldots, \sigma_r$ be the embeddings of $\mathbb{K}_1\mathbb{K}_2$ into $\mathbb{R}$. It follows immediately that the number of linearly independent matrices $\mathrm{diag}\{\sigma_1(uu^t), \ldots, \sigma_r(uu^t)\}$, $u \in \mathcal{M}(f_1 \otimes f_2)$, over $\mathbb{R}$ equals the number of linearly independent matrices uu^t, $u \in \mathcal{M}(f_1 \otimes f_2)$, over $\mathbb{Q}$.

Hence, the number of linearly independent matrices uu^t $(u \in \mathcal{M}(f_1 \otimes f_2))$ must be at least

$$N = r_1 r_2 \frac{m_1 m_2 (m_1 m_2 + 1)}{2}.$$

By hypothesis we obtain

$$\mathcal{L}_2(\mathcal{M}(f_1)) \otimes \mathcal{L}_2(\mathcal{M}(f_2)) \subseteq \mathcal{L}_2(\mathcal{M}(f_1 \otimes f_2)).$$

Hence $\dim \mathcal{L}_2(\mathcal{M}(f_1 \otimes f_2)) \geqslant N$. This proves that $f_1 \otimes f_2$ is perfect. □

Remark 2. Let ax^2 be a perfect unary quadratic form over a totally real algebraic number field $\mathbb{K}$. Since the principal perfect quadratic form ϕ_0 satisfies the hypothesis of Theorem 1 (by Theorem 7.1.2 in [11]), the perfect quadratic form $a\phi_0$ can be used as the initial perfect quadratic form in Voronoï's algorithm.

This motivates the study of perfect unary quadratic forms over totally real algebraic number fields.

On the other hand, if we have a perfect form of rank m over a totally real number field $\mathbb{K}$, then we can find all perfect forms (up to equivalence) of rank m over $\mathbb{K}$ by the generalization of Voronoï's algorithm. Among them there is a perfect

[1] See also Ch. 3, Proposition 17 in [12].

quadratic form $a\phi_0$ with a perfect unary form ax^2 over $\mathbb{K}$ and the principal perfect form ϕ_0 of rank m by Remark 2. Thus we can find all perfect quadratic forms over $\mathbb{K}$ (up to equivalence) by Theorem 1 and by applying the generalization of Voronoï's algorithm.

We conclude that in order to find all perfect forms (up to equivalence) over a totally real algebraic number field $\mathbb{K}$ it is sufficient to have an initial perfect quadratic form.

We have solved the problem of finding an initial perfect form for real quadratic algebraic number fields and partially for the maximal totally real subfield of cyclotomic fields.

Theorem 3 (Theorem 1 in $\left[{}^{13}\right]$). *Let $D > 1$ be a square-free integer.*

1. *Suppose that $|k^2 - D|$ attains a minimum at integer $k > 0$. If $D \equiv 2 \pmod 4$ or $D \equiv 3 \pmod 4$, then the unary form $ax^2 = (a_1 + a_2\sqrt{D})x^2$, with*
$$a_1 = 2kD, \qquad a_2 = k^2 + D - 1,$$
is perfect and $\{1, k - \sqrt{D}\} \subseteq \mathcal{M}(ax^2)$.
2. *Let $k > 0$ be the smallest integer such that $|(2k-1)^2 - D|$ is minimal. If $D \equiv 1 \pmod 4$, then the unary form $ax^2 = (a_1 + a_2\frac{1+\sqrt{D}}{2})x^2$, with*
$$a_1 = 1 - k^2 + (1+D)k - \frac{1+3D}{4}, \qquad a_2 = 2k^2 - 2k + \frac{1+D}{2} - 2,$$
is perfect and $\{1, -k + \frac{1+\sqrt{D}}{2}\} \subseteq \mathcal{M}(ax^2)$.

Theorem 4. *Let ζ_p be a primitive pth root of unity, where p is a prime. The unary quadratic form $(2 - \zeta_p - \zeta_p^{-1})x^2$ is a perfect quadratic form over $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Moreover, $\varepsilon \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*$ is a minimum vector of $(2 - \zeta_p - \zeta_p^{-1})x^2$ iff $\sigma(2 - \zeta_p - \zeta_p^{-1}) = (2 - \zeta_p - \zeta_p^{-1})\varepsilon^2$ holds for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p + \zeta_p^{-1})/\mathbb{Q})$.*

Applying Theorem 2, we obtain the following result.

Corollary 3. *Let $n > 1$ be a square-free odd integer $n = p_1 \cdots p_k$ and $3 \nmid n$. The unary quadratic form*
$$\left(\prod_{i=1}^{k}(2 - \zeta_{p_i} - \zeta_{p_i}^{-1})\right) x^2$$
is perfect over $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, where ζ_{p_i} is a primitive p_ith root of unity and ζ_n is a primitive nth root of unity.

The proofs will be published in near future.

4. EXTREME FORMS AND ADDITIVE HERMITE'S CONSTANT

Lemma 1. *Let $f = (f_i)_{i=1}^{r+s}$ and $g = (g_i)_{i=1}^{r+s}$ be nonproportional Humbert tuples of rank m over $\mathbb{K}$. Write $n = [\mathbb{K}\colon \mathbb{Q}]$. Then $F_t = (1-t)f + tg$ is a Humbert tuple and $\varphi(t) = d(F_t)^{1/mn}$ is a strictly concave function for all $t \in [0,1]$.*

Proof. Obviously $(1-t)f_i + tg_i$ is positive definite for all $t \in [0,1]$. Hence F_t is a Humbert tuple.

Denote by $\hat{f}$ and $\hat{g}$ the block-diagonal matrices $\mathrm{diag}\{f_1, \dots, f_{r+s}, \overline{f}_{r+1}, \dots, \overline{f}_{r+s}\}$ and $\mathrm{diag}\{g_1, \dots, g_{r+s}, \overline{g}_{r+1}, \dots, \overline{g}_{r+s}\}$, respectively. Let $\omega_1, \dots, \omega_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_\mathbb{K}$ and set

$$\mathcal{B} = \begin{pmatrix} \sigma_1(\omega_1)\mathrm{I}_m & \dots & \sigma_1(\omega_n)\mathrm{I}_m \\ & \cdots & \\ \sigma_n(\omega_1)\mathrm{I}_m & \dots & \sigma_n(\omega_n)\mathrm{I}_m \end{pmatrix},$$

where I_m denotes the identity matrix of m rows. Obviously the matrices $\overline{\mathcal{B}}^t \hat{f}\mathcal{B}$ and $\overline{\mathcal{B}}^t \hat{g}\mathcal{B}$ are positive definite over $\mathbb{R}$. Applying Theorem 4 of [14], Ch. 4, §12, we get an invertible matrix T such that

$$T^t\overline{\mathcal{B}}^t \hat{f}\mathcal{B}T = \mathrm{diag}\{1, \dots, 1\},$$

$$T^t\overline{\mathcal{B}}^t \hat{g}\mathcal{B}T = \mathrm{diag}\{\beta_1, \dots, \beta_{nm}\}.$$

Hence,

$$d(F_t) = \frac{1}{|\det(\mathcal{B})|^2} d((1-t)\hat{f} + t\hat{g}) = \frac{1}{|\det(\mathcal{B})|^2} \prod_{k=1}^{nm} (1 - t + t\beta_k)$$

and

$$\frac{\mathrm{d}^2}{(\mathrm{d}t)^2} \log(d(F_t)) = -\sum_{k=1}^{nm} \left(\frac{\beta_k - 1}{1 - t + t\beta_k} \right)^2 < 0.$$

Since $\log$ is a concave function, we have also that $d(F_t)$ is a concave function and so is $\varphi(t) = d(F_t)^{1/nm}$. □

Let $\langle \cdot, \cdot \rangle$ be a symmetric positive definite bilinear form on the $\mathbb{R}$-vector space

$$X = \prod_{i=1}^{r} \mathbb{R}^{m(m+1)/2} \times \prod_{i=1}^{s} \mathbb{R}^{m^2},$$

(X is spanned by Humbert tuples over $\mathbb{K}$) such that $\langle f, g \rangle > 0$ for all $f \in \mathcal{P}_{m,\mathbb{K}}$ and $g \in \overline{\mathcal{P}_{m,\mathbb{K}}}$. Let D be a discrete set in $\overline{\mathcal{P}_{m,\mathbb{K}}} \setminus \{0\}$, that is, an arbitrary compact set $K \subset \overline{\mathcal{P}_{m,\mathbb{K}}} \setminus \{0\}$ contains only finitely many points of D. For each $f \in \mathcal{P}_{m,\mathbb{K}}$ we let (see [1], p. 389)

$$\mu(f) = \mu_D(f) = \inf\{\langle f, y \rangle | y \in D\}.$$

Lemma 2 (Lemma 3 in [1]). *For each $f \in \mathcal{P}_{m,\mathbb{R}}$ and $\varepsilon > 0$ there exists a neighbourhood $\mathcal{U} \subset \mathcal{P}_{m,\mathbb{K}}$ of f such that*

$$\mathcal{M}(g) \subseteq \mathcal{M}(f) \qquad \textit{and} \qquad |\mu(g) - \mu(f)| < \varepsilon$$

for all $g \in \mathcal{U}$.

For the rest of the paper we fix $D = \{v\bar{v}^t | v \in \mathcal{O}_{\mathbb{K}}^m \setminus \{0\}\}$ and $\langle f, v\bar{v}^t \rangle = \mathrm{Tr} f(v)$.

Theorem 5. *The extreme Humbert tuple f over $\mathbb{K}$ is perfect and weakly eutactic.*

Proof. Seeking a contradiction, suppose that the extreme Humbert tuple $f = (f_{\sigma_i})_{i=1}^{r+s}$ is not perfect. Due to Lemma 2 there exists a neighbourhood $\mathcal{U} \subset \mathcal{P}_{m,\mathbb{K}}$ such that $\mathcal{M}(g) \subseteq \mathcal{M}(f)$ for all $g \in \mathcal{U}$. Fix a Humbert tuple $g \in \mathcal{U}$ that is not proportional to f. Without loss of generality, we assume that $\mu(g) = \mu(f)$. Let

$$F_\rho = (1 - \rho) f + \rho g$$

be a Humbert tuple with

$$F_\rho^{(k)} = (1 - \rho) f_k + \rho g_k$$

at the kth position for each $k = 1, \ldots, r + s$. One can choose a real number ρ_0 such that $F_\rho^{(k)}$ is positive definite for all $1 \leq k \leq r + s$ and $\rho \in (-\rho_0, \rho_0)$. Using the extremality, one has

$$\frac{\mu(F_\rho)}{d(F_\rho)^{1/nm}} \leq \frac{\mu(f)}{d(f)^{1/nm}} = \frac{\mu(F_0)}{d(F_0)^{1/nm}}$$

and there exists a minimal vector $u = (u_1, \ldots, u_m)$ such that

$$d(F_\rho)^{-1/nm} \langle f + \rho(g - f), u\bar{u}^t \rangle \leq d(f)^{-1/nm} \langle f, u\bar{u}^t \rangle \quad \forall \rho \in (-\rho_0, \rho_0).$$

Since $\mu(f) = \mu(g)$, i.e. $\langle g - f, u\bar{u}^t \rangle = 0$, we have

$$d(F_\rho)^{-1/nm} \langle f, u\bar{u}^t \rangle \leq d(f)^{-1/nm} \langle f, u\bar{u}^t \rangle \quad \forall \rho \in (-\rho_0, \rho_0).$$

Cancelling out the equal term, we obtain $d(F_\rho) \geq d(f)$ for all $\rho \in (-\rho_0, \rho_0)$. Hence the continuous function $\mathbb{R} \to \mathbb{R}$, $\rho \rightsquigarrow d(F_\rho)$ has a local minimum at $\rho = 0$. This gives a contradiction to Lemma 1. Hence f is perfect.

Let us show that f is weakly eutactic. Without loss of generality, we assume that $\det(f_k) = 1$ for all $1 \leq k \leq r + s$. (Obviously f is weakly eutactic iff $\alpha f = (\alpha_1 f_1, \ldots, \alpha_{r+s} f_{r+s})$, $\alpha \in (\mathbb{R}_{>0})^{r+s}$, is weakly eutactic.) We write $\mathrm{TR}(*)$ for the trace of a matrix $*$. If H and H' are both either symmetric $m \times m$ matrices over $\mathbb{R}$ or complex $m \times m$ Hermitian matrices, then we denote

$$\langle H, H' \rangle_\bullet = \mathrm{TR}(H\overline{H'}).$$

We identify the space of $m \times m$ symmetric matrices by $\mathbb{R}^{m(m+1)/2}$ and the space of complex $m \times m$ Hermitian matrices by $\mathbb{R}^{m^2}$ in the natural way. For a fixed nonzero tuple $g = (g_1, \dots, g_{r+s})$ of real $m \times m$ symmetric matrices $g_1, \dots, g_r$ and complex $m \times m$ Hermitian matrices $g_{r+1}, \dots, g_{r+s}$, we define the following linear half-spaces:

$$\Psi_k = \{(\xi_{k,ij}) \in \mathbb{R}^{m(m+1)/2} \mid \langle (g_{k,ij}), (\xi_{k,ij}) \rangle_\bullet \geq 0,\ \xi_{k,ij} = \xi_{k,ji}\},$$

$$\Psi_k = \{(\xi_{k,ij}) \in \mathbb{R}^{m^2} \mid \langle (g_{k,ij}), (\xi_{k,ij}) \rangle_\bullet \geq 0,\ \xi_{k,ij} = \overline{\xi_{k,ji}}\}.$$

Suppose that Ψ_k contains the point which represents the semidefinite form $\sigma_k(u)\sigma_k(u)^t$ if $1 \leq k \leq r$ or $\sigma_k(u)\overline{\sigma_k(u)}^t$ if $r+1 \leq k \leq r+s$ for all $u \in \mathcal{M}(f)$.

Let $r < k_0 \leq k+s$. Consider the forms

$$F_\rho^{(k)} = f_k \quad \text{if } k \neq k_0,$$

$$F_\rho^{(k)} = (f_k + \rho g_k) \quad \text{if } k = k_0.$$

The tuple $F_\rho = (F_\rho^{(k)})_{k=1}^{r+s}$ is a Humbert tuple for ρ small enough. Moreover, we can assume that the inequality

$$d(F_\rho)^{-1/nm}\mu(F_\rho) \leq d(f)^{-1/nm}\mu(f)$$

holds for this ρ. Suppose $v \in \mathcal{M}(f) \cap \mathcal{M}(F_\rho)$ (such v exists by Lemma 2). Then

$$d(F_\rho)^{-1/nm}\left(\langle f, v\bar{v}^t\rangle + 2\rho\langle g_{k_0}, \sigma_{k_0}(v\bar{v}^t)\rangle_\bullet\right) \leq d(f)^{-1/nm}\langle f, v\bar{v}^t\rangle.$$

Also, for a suitably chosen small positive ρ we have

$$d(F_\rho)^{-1/nm}\left(\langle f, v\bar{v}^t\rangle + 2\rho\langle g_{k_0}, \sigma_{k_0}(v\bar{v}^t)\rangle_\bullet\right) \geq d(F_\rho)^{-1/nm}\langle f, v\bar{v}^t\rangle,$$

due to the assumption $\langle g_{k_0}, \sigma_{k_0}(v\bar{v}^t)\rangle_\bullet \geq 0$. Putting those inequalities together and cancelling out equal terms, we obtain the inequality $\det(f_{k_0}) \leq \det(F_\rho^{(k_0)})$. It follows from Lemma 1 that

$$\frac{\mathrm{d}}{\mathrm{d}\rho}\left(\det(F_\rho^{(k_0)})\right)\Big|_{\rho=0} > 0.$$

Expanding the derivative, we find

$$\frac{\mathrm{d}}{\mathrm{d}\rho}\left(\det(F_\rho^{(k_0)})\right)\Big|_{\rho=0} = \sum_{ij} g_{k_0,ij}\frac{\partial}{\partial f_{k_0,ij}}\left(\det(f_{k_0})\right) = \sum_{ij} g_{k_0,ij} f^*_{k_0,ij}.$$

Here $f^*_{k_0}$ denotes the dual form of f_{k_0}. Hence, the point in $\mathbb{R}^{m^2}$ corresponding to the Hermitian form $f^*_{k_0}$ lies in the interior of any linear half-space Ψ_{k_0} that contains the points representing the form $(\sigma_{k_0}(u)\cdot\mathbf{x})\overline{(\sigma_{k_0}(u)\cdot\mathbf{x})}$ for all $u \in \mathcal{M}(f)$. Therefore it lies in the interior of the convex hull in $\mathbb{R}^{m^2}$, determined by the forms $(\sigma_{k_0}(u)\cdot\mathbf{x})\overline{(\sigma_{k_0}(u)\cdot\mathbf{x})}$, $u \in \mathcal{M}(f)$.

The argumentation is similar for quadratic forms, i.e. for real embeddings of $\mathbb{K}$ (see [5], pp. 20–21). □

Combining Corollary 2 with the last theorem, we obtain the following corollary.

Corollary 4. *If f is an extreme Humbert tuple over totally real or totally complex $\mathbb{K}$ and f has a rational minimum λ_1, then f is a conjugate tuple.*

Using the properties of extreme Humbert tuples, it is possible to give some estimates for bounds of the additive Hermite's constant. Hermite's constant (for quadratic forms over rational numbers) is denoted by γ_ℓ (i.e. the notation of the number field is omitted in the subscript).

Theorem 6. *For any algebraic number field $\mathbb{K}$ and for any $m \geq 1$ we have the upper bound*

$$\gamma_{m,\,\mathbb{K}} \leq \gamma_{m\cdot[\mathbb{K}\colon\,\mathbb{Q}]}|\mathrm{disc}(\mathbb{K})|^{1/[\mathbb{K}\colon\,\mathbb{Q}]}. \tag{3}$$

Proof. Let $f = (f_1, \ldots, f_{r+2s})$ be a conjugate tuple. Applying matrix $\mathcal{B}$ to $\hat{f} = \mathrm{diag}\{f_1, \ldots, f_{r+2s}\}$, we get a positive definite quadratic form F over $\mathbb{Q}$ such that

$$\min\{F(X)|\ X \in \mathbb{Z}^{m\cdot[\mathbb{K}\colon\,\mathbb{Q}]} \setminus \{0\}\} = \min\{\mathrm{Tr}(f(X))|X \in \mathcal{O}_{\mathbb{K}}^m \setminus \{0\}\}.$$

Hence

$$\begin{aligned}
\gamma_{\mathbb{K}}(f) &= \frac{\min\{\mathrm{Tr}(f(X))|X \in \mathcal{O}_{\mathbb{K}}^m \setminus \{0\}\}}{d(f)^{1/m\cdot[\mathbb{K}\colon\,\mathbb{Q}]}} \\
&= \frac{\min\{F(X)|\ X \in \mathbb{Z}^{m\cdot[\mathbb{K}\colon\,\mathbb{Q}]} \setminus \{0\}\}}{\det(F)^{1/m\cdot[\mathbb{K}\colon\,\mathbb{Q}]}}\ \det(\mathcal{B})^{2/[\mathbb{K}\colon\,\mathbb{Q}]} \\
&= \gamma_{\mathbb{Q}}(F) \cdot |\mathrm{disc}(\mathbb{K})|^{1/[\mathbb{K}\colon\,\mathbb{Q}]} \\
&\leq \gamma_{m\cdot[\mathbb{K}\colon\,\mathbb{Q}]} \cdot |\mathrm{disc}(\mathbb{K})|^{1/[\mathbb{K}\colon\,\mathbb{Q}]}.
\end{aligned}$$ □

This is the best upper bound. For example, the upper bound is attained for $\gamma_{1,\,\mathbb{Q}(\sqrt{3})}$, $\gamma_{2,\,\mathbb{Q}(\sqrt{2})}$, and $\gamma_{2,\,\mathbb{Q}(\sqrt{3})}$. The last two cases can be verified immediately using the results of Ong [2,3]. However, the explicit values of γ_ℓ are known only for $2 \leq \ell \leq 8$ [15].

The following corollary follows immediately from Theorem 6.

Corollary 5. *Let f be a positive quadratic form over an algebraic number field $\mathbb{K}$. If the rational quadratic form $\mathrm{Tr} f$ is critical over $\mathbb{Q}$, then f is critical over $\mathbb{K}$.*

Let $\gamma_{m,\mathbb{K}}^*$ denote the Hermite–Humbert constant introduced by Icaza (see [5]).

Proposition 4. *For any algebraic number field $\mathbb{K}$ of degree n over $\mathbb{Q}$, we have*

$$\gamma_{m,\mathbb{K}} \geqslant n\sqrt[n]{\gamma_{m,\mathbb{K}}^*}.$$

Proof. Let f be a Humbert tuple of rank m such that

$$\gamma^*_{m,\mathbb{K}} = \frac{\min\{\mathrm{Nm} f(X) | X \in \mathcal{O}^m_{\mathbb{K}} \setminus \{0\}\}}{\sqrt[m]{d(f)}}.$$

This tuple exists by Theorem 2 of [5]. Let $0 \neq y \in \mathcal{O}^m_{\mathbb{K}}$ be a trace minimum vector of f. Applying the inequality between arithmetic and geometric means, we have

$$\mathrm{Tr} f(y) \geqslant n \sqrt[n]{\mathrm{Nm} f(y)} \geqslant n \sqrt[n]{\min\{\mathrm{Nm} f(X) | X \in \mathcal{O}^m_{\mathbb{K}} \setminus \{0\}\}}.$$

From this we obtain

$$n \cdot \sqrt[n]{\gamma^*_{m,\mathbb{K}}} \leqslant \frac{\min\{\mathrm{Tr} f(X) | X \in \mathcal{O}^m_{\mathbb{K}} \setminus \{0\}\}}{d(f)^{1/nm}} \leqslant \gamma_{m,\mathbb{K}}. \qquad \square$$

5. TWO EXAMPLES

Let ζ_n be a primitive nth root of unity. To shorten the notation, we write θ_n instead of $\zeta_n + \zeta_n^{-1}$.

Example 2. Let $\mathbb{K} = \mathbb{Q}(\theta_9)$ and consider the positive definite binary quadratic form $f(x, y) = (1 + \theta_9)^2(x^2 + \theta_9 xy + y^2)$. One immediately verifies that $\gamma_{\mathbb{K}}(f)$ attains the upper bound given in Theorem 6. Hence f is critical over $\mathbb{K}$.

Taking the trace form of f, we obtain the critical senary quadratic form E_6 (cf. Section 4.5 in [9]) over $\mathbb{Q}$.

Example 3. Similarly, let $\mathbb{K} = \mathbb{Q}(\theta_{20})$ and consider $f(x, y) = (\theta_{20} + \theta_{20}^2)(x^2 + \theta_{20} xy + y^2)$. Arguing as in the previous example, we obtain that f is a critical quadratic form. Hence, $\gamma_{\mathbb{K}}(f)$ gives the upper bound (3) and $\mathrm{Tr} f(X)$ is equivalent to E_8 (cf. Section 4.4 in [9]), since $\mathrm{Tr} f(X)$ is a critical quadratic form of rank 8 over $\mathbb{Q}$.

The algebraic construction of those two quadratic forms $\mathrm{Tr} f(X)$ is the construction of Craig [16] in terms of a trace function.

One can easily verify that the unary quadratic forms $(1 + \theta_9)^2 x^2$ and $(\theta_{20} + \theta_{20}^2)x^2$ are perfect over the number fields $\mathbb{Q}(\theta_9)$ and $\mathbb{Q}(\theta_{20})$, respectively (see also [17]). Denote by

$$\phi_0^{(m)}(x_1, \ldots, x_m) = \sum_{i=1}^m x_i^2 + \sum_{i=1}^m \sum_{j=i+1}^m x_i x_j$$

the initial rational perfect form of rank m. Thus, for each $m > 0$ the initial perfect forms over the number fields $\mathbb{Q}(\theta_9)$ and $\mathbb{Q}(\theta_{20})$ are $(1 + \theta_9)^2 \phi_0^{(m)}$ and $(\theta_{20} + \theta_{20}^2)\phi_0^{(m)}$, respectively, by Theorem 1.

6. OPEN PROBLEMS

The main open problem is the generalization of eutaxy for a quadratic form over algebraic number fields. Weak eutaxy (see Definition 5) is not enough for generalizing sufficient conditions of the well-known Voronoï's theorem.

ACKNOWLEDGEMENTS

I thank Prof. Paul Tammela for the valuable discussions and comments on this paper. I also thank two anonymous referees for the useful suggestions and remarks. This research was partially supported by the Estonian Science Foundation (grant No. 4291).

REFERENCES

1. Koecher, M. Beiträge zu einer Reduktionstheorie in Positivitätsbereichen I. *Math. Ann.*, 1960, **141**, 384–432.
2. Ong, H. E. *Volkommene quadratische Formen über reellquadratischen Zahlkörpern*. PhD thesis, Frankfurt, 1983.
3. Ong, H. E. Perfect quadratic forms over real quadratic number fields. *Geom. Dedicata*, 1986, **20**, 51–77.
4. Baeza, R. and Icaza, M. I. On Humbert–Minkowski's constant for a number field. *Proc. Am. Math. Soc.*, 1997, **125**, 3195–3202.
5. Icaza, M. I. Hermite constant and extreme forms. *J. London Math. Soc.*, 1997, **55**, 11–22.
6. Coulangeon, R. Voronoï theory over algebraic number fields. In *Réseaux euclidiens, designs sphériques et formes modulaires* (Martinet, J., ed.). *Monogr. Enseign. Math.*, 2001, 37, 147–162.
7. Koecher, M. Beiträge zu einer Reduktionstheorie in Positivitätsbereichen II. *Math. Ann.*, 1961, **144**, 175–182.
8. Gruber, P. M. and Lekkerkerker, C. G. *Geometry of Numbers*. North-Holland, Amsterdam, 1987.
9. Martinet, J. *Perfect Lattices in Euclidean Spaces*. Grundlehren der mathematischen Wissenschaften, Vol. 327. Springer-Verlag, Heidelberg, 2003.
10. Baeza, R., Coulangeon, R., Icaza, M. I. and O'Ryan, M. Hermite's constant for quadratic number fields. *Exp. Math.*, 2001, **10**, 543–551.
11. Kitaoka, Y. *Arithmetic of Quadratic Forms*. Cambridge University Press, Cambridge, 1993.
12. Lang, S. *Algebraic Number Theory. Second Edition*. Graduate Texts in Mathematics, Vol. 10. Springer-Verlag, Heidelberg, 1994.
13. Leibak, A. The complete enumeration of binary perfect forms over the algebraic number field $\mathbb{Q}(\sqrt{6})$. *Proc. Estonian Acad. Sci. Phys. Math.*, 2005, **54**, 212–234.
14. Bellmann, R. *Introduction to Matrix Analysis*. McGraw Hill, New York, 1960.
15. Ohno, S. and Watanabe, W. Estimates of Hermite constants for algebraic number fields. *Comm. Mat. Univ. St. Pauli*, 2001, **50**, 53–63.
16. Craig, M. Extreme forms and cyclotomity. *Mathematika*, 1978, **25**, 44–56.
17. Sigrist, F. Cyclotomic quadratic forms. *J. Théor. Nombres Bordeaux*, 2000, **12**, 519–530.

Voronoï teooria aditiivsest üldistusest algebralistele arvukorpustele

Alar Leibak

On uuritud täiuslike ruutvormide Voronoï teooria aditiivset üldistust algebralistele arvukorpustele, kus positiivselt määratud ruutvormide või Hermite'i vormide asemel on vaadeldud Humberti korteeže. On näidatud, et aditiivse üldistuse mõttes piisab, kui vaadelda ainult erikujulisi Humberti korteeže (lause 2). On tõestatud täiuslike vormide omadusi ja konstruktsioone, kuidas saada olemasolevatest täiuslikest vormidest uusi täiuslikke vorme (lause 2, teoreemid 1 ja 2).

On üldistatud Voronoï teoreemi (st ekstremaalse ruutvormi tarvilik ja piisav tingimus) tarvilik tingimus algebralistele arvukorpustele (teoreem 5).