On the Computation of the Norm-Euclidean Minimum of Algebraic Number Fields

Michele Elia
Dipartimento di Elettronica
Politecnico di Torino
I-10129 Torino, Italy
elia@polito.it

J. Carmelo Interlando
Department of Mathematics and Statistics
San Diego State University, San Diego, CA, USA
carmelo.interlando@sdsu.edu

Abstract
Let $\mathbb{F}$ be an algebraic number field whose group of units has rank $\geq 1$. The conjecture that the norm-Euclidean minimum $M(\mathbb{F})$ is a rational number is affirmatively settled. It is proved that $M(\mathbb{F})$ is lower bounded by the inverse of the smallest norm of all nonzero prime $\mathfrak{O}_F$-ideals. Furthermore, when $\mathbb{F}/\mathbb{Q}$ is a normal extension, the numerator and denominator of $M(\mathbb{F})$ lie within finite sets of integers that can be explicitly calculated. As an application, it is proved that the known lower bounds of $M(\mathbb{F})$ for the cyclotomic field $\mathbb{Q}(\zeta_5)$ and the cyclic cubic fields of discriminants $103^2$, $109^2$, $117^2$, and $157^2$ are the actual values of $M(\mathbb{F})$.

Mathematics Subject Classification: 11R04, 13F07, 13A05, 11R27, 11Y40

Keywords: algebraic number fields, Euclidean rings, units, group actions

I Introduction

The problem of establishing whether an algebraic number field is a Euclidean domain has always attracted a lot of interest [6]. The Euclidean character of fields has been considered with respect to many different norms, with prevalence of the absolute value of the field norm. In this paper, $\mathbb{F}$ denotes an algebraic number field defined by a monic irreducible polynomial $f(x)$ of degree $n$ in $\mathbb{Z}[x]$. As customary, $\mathfrak{O}_F$ denotes the ring of integers of $\mathbb{F}$. We say that $\mathbb{F}$ is norm-Euclidean if its ring of integers $\mathfrak{O}_F$ is a Euclidean domain for $|N_\mathbb{F}(.)|$, 

the absolute value of the field norm relative to \( \mathbb{Q} \). That is, given \( \alpha, \beta \in \mathcal{O}_F \), there exist \( \theta, \nu \in \mathcal{O}_F \) such that \( \alpha = \theta \beta + \nu \) with \( |N_{\mathbb{Q}}(\nu)| < |N_{\mathbb{Q}}(\beta)| \). Most of the proofs concerning Euclidean domains are based on the following proposition, which is a consequence of the results contained in [5, Section 14.7, p. 212]:

**Proposition 1.** The number field \( F \) is norm-Euclidean if and only if for every \( \alpha \in F \), there exists \( \beta \in \mathcal{O}_F \) such that \( |N_{\mathbb{Q}}(\alpha - \beta)| < 1 \).

The norm-Euclidean minimum of \( F \), denoted by \( M(F) \), is defined in [6] as

\[
M(F) = \sup_{\xi \in F} \inf_{\nu \in \mathcal{O}_F} |N_{\mathbb{Q}}(\xi - \nu)|. \tag{1}
\]

Note that \( F \) is norm-Euclidean or not according to whether \( M(F) < 1 \) or \( M(F) > 1 \), respectively. If \( M(F) = 1 \), then both possibilities can occur, see [6].

In [12], van der Linden proved that \( M(F) \) is achievable if \( F \) has unit rank 1, that is, an element \( \xi_0 \) in \( F \) exists such that \( M(F) = |N_{\mathbb{Q}}(\xi_0)| \), which implies that \( M(F) \in \mathbb{Q} \). In [6], the Euclidean properties of number fields are surveyed and some surmises [6, p. 4] are put forth. In particular, it is conjectured that if \( F \) has unit rank \( \geq 1 \) then:

i) \( M(F) \) is achievable in \( F \);

ii) \( M(F) = \frac{a}{d} \) where \( a, d \in \mathbb{Z} \).

These conjectures are supported, or at least not contradicted, by Lemmermeyer’s extended tables [6] of number fields of given discriminant listed along with known or supposed norm-Euclidean minima.

Norm-Euclidean quadratic fields have been completely classified, see [6, Section 4] for the succession of events that led to it. More specifically, \( \mathbb{Q}(\sqrt{m}) \) is norm-Euclidean if and only if \( m \) is one of the 21 integers: \(-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\).

In this paper, conjectures i) and ii) are affirmatively settled by extending an action of the unit group of \( F \) on \( F/\mathcal{O}_F \) to \( \mathbb{R}^n \). That group action was considered by Barnes and Swinnerton-Dyer [6]. As a consequence, it is shown that \( M(F) \) is lower bounded by the inverse of the smallest norm of all nonzero prime \( \mathcal{O}_F \)-ideals. Furthermore, it is shown that in numerical evaluations of \( M(F) = \frac{a}{d} \), the denominator \( d \) is taken from a finite set of integers which depends on the fundamental units of \( F \). This set is explicitly defined for any \( F \) which is a normal extension of \( \mathbb{Q} \) and has a group of units of rank greater than zero. Lastly, previously unknown values of \( M(F) \) for fields of small degree and discriminant are given in Table 1.
II Preliminaries

Given an integral basis \( \{ \omega_1, \ldots, \omega_n \} \) for \( F \), any \( \xi \in F \) can be represented either by a vector \( \phi(\xi) \) in \( \mathbb{Q}^n \) or by an \( n \times n \) matrix \( D(\xi) \) with rational entries. The relation

\[
\xi = \sum_{i=1}^{n} x_i \omega_i, \quad x_i \in \mathbb{Q},
\]

defines a bijective mapping \( \phi : F \to \mathbb{Q}^n \) where for any \( \xi \in F \), \( \phi(\xi) = (x_1, x_2, \ldots, x_n)^T \in \mathbb{Q}^n \). It follows that \( \phi(F) = \mathbb{Q}^n \) and \( \phi\left(\mathcal{O}_F\right) = \mathbb{Z}^n \). A representation of \( F \) by matrices is defined by

\[
D(\xi) = \sum_{i=1}^{n} x_i D(\omega_i), \quad x_i \in \mathbb{Q},
\]

where \( D(\omega_i) = (d_{ij}^{(i)}) \) are integral matrices, see [14, pp. 1-3]. For \( i = 1, \ldots, n \), the matrix \( D(\omega_i) \) is defined by the action of \( \omega_i \) on the row vector \( \Omega = (\omega_1, \ldots, \omega_n) \) as

\[
\omega_i \omega_h = \sum_{j=1}^{n} d_{jh}^{(i)} \omega_j, \quad 1 \leq h \leq n,
\]

that is, \( \omega_i \Omega = \Omega D(\omega_i) \). Note that \( D \) is a ring monomorphism from \( F \) into the ring \( \mathbb{M}(n, \mathbb{Q}) \) of \( n \times n \) rational matrices. It follows, with some abuse of notation, that \( D(F) \subseteq \mathbb{M}(n, \mathbb{Q}) \) and \( D(\mathcal{O}_F) \subseteq \mathbb{M}(n, \mathbb{Z}) \).

Let \( \sigma_1, \ldots, \sigma_n \) be the embeddings of \( F \) in \( \mathbb{C} \), that is, the \( \mathbb{Q} \)-isomorphisms of \( F \) in \( \mathbb{C} \). Then the eigenvalues of \( D(\xi) \) are \( \xi \) and its conjugates, that is, \( \sigma_1(\xi), \ldots, \sigma_n(\xi) \), since

\[
\Omega D(\xi) = \Omega \sum_{i=1}^{n} x_i D(\omega_i) = \sum_{i=1}^{n} x_i \Omega D(\omega_i) = \sum_{i=1}^{n} x_i \omega_i \Omega = \xi \Omega,
\]

and \( \sigma_j(D(\xi)) = D(\xi) \) because the entries in \( D(\xi) \) are rational numbers. Using \( \phi \) and \( D \), the field product, trace, and norm are computed in \( F \) as:

\[
\phi(\xi \eta) = D(\eta) \phi(\xi) = D(\xi) \phi(\eta), \quad \text{Tr}_F(\xi) = \text{tr}(D(\xi)), \quad \text{and} \quad N_F(\xi) = \det(D(\xi)),
\]

respectively.

A complex number \( z \) of the form \( \sum_{i=1}^{n} x_i \omega_i \) where the \( x_i \) are rational or real numbers and at least one of the \( x_i \) belongs to \( \mathbb{R} \setminus \mathbb{Q} \) will be called an irrational point of \( F \). The representation \( \phi(z) \) of \( z \) is not unique, but for our purposes this fact is irrelevant. The irrational points of \( F \) do not belong to \( F \), but they may be viewed as limit points of sequences of elements of \( F \). The union of \( F \) and its irrational points will be denoted by \( \overline{F} \).

Note that the representations \( \phi \) and \( D \) can be both extended to \( \overline{F} \) in the obvious way.

Let \( \mathbb{H}_n \) be the hypercube \( \{(x_1, \ldots, x_n) \mid 0 \leq x_i < 1\} \) with vertex set \( V_n = \{(x_1, \ldots, x_n) \mid x_i \in \{0, 1\}\} \). Note that \( \mathbb{H}_n \) is the fundamental region \( F_n \) of the lattice \( \phi(\mathcal{O}_F) = \mathbb{Z}^n \). The image \( \mathbb{T}_n = \phi(F/\mathcal{O}_F) \) is the set of points in \( \mathbb{H}_n \) with rational coordinates.
**Definition 1.** Given any point $\xi$ of $\mathbb{F}$, its distance $\text{dist}(\xi, \mathcal{O}_F)$ from the ring of integers $\mathcal{O}_F$ is defined as

$$\text{dist}(\xi, \mathcal{O}_F) = \inf_{\nu \in \mathcal{O}_F} |N_F(\xi - \nu)|.$$ 

Similarly, for any $\delta \in \mathcal{O}_F$, the distance between $\xi$ and the integral $\mathcal{O}_F$-ideal $\delta \mathcal{O}_F$ is defined as $\text{dist}(\xi, \delta \mathcal{O}_F) = \inf_{\nu \in \mathcal{O}_F} |N_F(\xi - \delta \nu)|$. Although we will not be doing explicit calculations with irrational points, Definition 1 can be extended to irrational points $z \in \mathbb{F}$ with the assumption of referring to a specific representation $\phi(z)$. The distance of an irrational point $z$ to $\mathcal{O}_F$ is then defined as the infimum of the distances over all possible representations of $z$.

**Definition 2.** A rational or irrational point $\xi_o \in \mathbb{F}$ is said to be optimal if

$$\text{dist}(\xi_o, \mathcal{O}_F) = \sup_{\phi(\xi) \in \mathbb{R}^n} \text{dist}(\xi, \mathcal{O}_F) = M(\mathbb{F}) = |N_F(\xi_o)|.$$ 

A rational or irrational optimal point $\xi_o$ is called a 0-optimal point if $M(\mathbb{F}) = \text{dist}(\xi_o, \mathcal{O}_F) = |N_F(\xi_o)|$.

Note that the search for the supreme can be restricted to points $\xi \in \mathbb{F}$ such that $\phi(\xi) \in \mathbb{H}^n$ since $\text{dist}(\xi, \mathcal{O}_F)$ is defined modulo $\mathcal{O}_F$. A 0-optimal point $\xi_o \in \mathbb{F}$ can always be found since $|N_F(\cdot)|$ is a continuous function from $\mathbb{R}$ into $\mathbb{R}^+$, the set of nonnegative real numbers, see [6, p. 7]. In other words, some rational or irrational optimal point $\xi_o$ is always achievable.

For $\delta \in \mathcal{O}_F$, let $\mathcal{O}(\delta) = \mathcal{O}_F/\delta \mathcal{O}_F$ denote the residue class ring modulo $\delta$ [3, pp. 24-31]. The multiplicative subgroup of the elements prime with $\delta$ in $\mathcal{O}(\delta)$ is denoted by $\mathcal{T}(\delta)^*$. The order of $\mathcal{T}(\delta)$ is equal to the absolute value of the field norm of $\delta$, that is, $|\mathcal{T}(\delta)| = |N_F(\delta)|$. The order of $\mathcal{T}(\delta)^*$ is equal to the Euler totient function $\varphi(\delta)$ counting the number of algebraic integers that are units in the ring $\mathcal{O}_F/\delta \mathcal{O}_F$, see [2, p. 231, Problem 4] for its properties. The function $\varphi(\delta)$ can be computed from the prime-power factorization of $\delta = \prod_{i=1}^{s} \beta_i^{\ell_i}$ in $\mathcal{O}_F$. More specifically,

$$\varphi(\delta) = N_F(\delta) \prod_{i=1}^{s} \left(1 - \frac{1}{N_F(\beta_i)}\right), \quad (3)$$

see [2, p. 231, Problem 5] or [8, p. 152].

Let $\mathcal{U}(\mathbb{F})$ be the group of units of $\mathcal{O}_F$. With some abuse of language, we will also refer to $\mathcal{U}(\mathbb{F})$ as the group of units of $\mathbb{F}$. Define $\psi_\delta : \mathcal{O}_F \to \mathcal{T}(\delta)$ as the homomorphism that maps every element $\alpha \in \mathcal{O}_F$ into the coset $\alpha + \delta \mathcal{O}_F$ that contains it. Thus, $\psi_\delta(\mathcal{U}(\mathbb{F}))$ is a finite subgroup of $\mathcal{T}(\delta)^*$ having index $s$, the order of the quotient group $\mathcal{T}(\delta)^*/\psi_\delta(\mathcal{U}(\mathbb{F}))$. Note that $s$ can be any factor of $\varphi(\delta)$, including 1.

The group of units $\mathcal{U}(\mathbb{F}) = E(\mathbb{F}) \times U(\mathbb{F})$ is the direct product of a finite cyclic group $E(\mathbb{F})$ of order $2m$, with $m$ a divisor of discriminant of $\mathbb{F}$ [9, Proposition 3.11, p. 97], and an infinite free group $U(\mathbb{F})$ of rank $r$, which is isomorphic to the direct product of $r$ copies of the additive group $\mathbb{Z}$. By Dirichlet’s Unit Theorem [8, p. 114], $r = r_1 + r_2 - 1$ where $[r_1, r_2]$ is the signature of $\mathbb{F}$. 

---

M. Elia and J. Carmelo Interlando
III Orbits

Barnes and Swinnerton-Dyer made use of an \( \mathcal{U}(F) \)-action on \( T_n = \phi(F/D_F) \) to describe many norm properties of \( F \), [6]. In this section the \( \mathcal{U}(F) \)-action is used to define a mapping \( \Phi_u \) from \( F \) into \( T_n \) for every \( u \in \mathcal{U}(F) \), which is directly extended to a mapping from \( F \) into \( H_n \). Thus \( \Phi_u \) is restricted to specify a one-to-one mapping from \( F/D_F \) into \( T_n \), or from \( F/D_F \) into \( H_n \). In what follows, the notation \( \lfloor x \rfloor \) is used to indicate the vector in \( \mathbb{R}^n \) whose entries are the greatest integers less than or equal to the entries in the vector \( x \in \mathbb{R}^n \).

**Definition 3.** For any \( u \in \mathcal{U}(F) \), let \( \Phi_u : F \to T_n \) be the mapping defined by

\[
\Phi_u(\xi) = D(u)\phi(\xi) - \lfloor D(u)\phi(\xi) \rfloor, \tag{4}
\]

for all \( \xi \in F \). We will use the same notation to denote the obvious extension of \( \Phi_u \) to a map from \( F \) to \( H_n \). The set \( \mathcal{C}_u(\xi) = \{\Phi_u(\xi) ; u \in \mathcal{U}(F)\} \subset H_n \) is called the orbit of \( \xi \in F \) by the action of \( \mathcal{U}(F) \). The orbit length is the cardinality \( |\mathcal{C}_u(\xi)| \) if \( |\mathcal{C}_u(\xi)| < \infty \); otherwise, the orbit is said to be of infinite length.

For our purposes, \( \Phi_u \) will be conveniently restricted to a mapping \( \Phi_u : F/D_F \to T_n \) without any loss. The use of the same notation does not cause any confusion since the action of \( \Phi_u \) on \( F \) is a projection of \( F \) into \( T_n \).

**Remark 1.** Let \( \xi = \frac{\varphi}{\delta} \in F \) be a rational point of \( F \), with \( \eta \) and \( \delta \) relatively prime integers in \( D_F \). Therefore, the operations related to the computation of \( \Phi_u(\xi) \) with fixed \( \delta \) can be described in terms of modular operations. It is immediately seen that \( \Phi_u(\frac{\eta + \lambda}{\delta}) = \Phi_u(\frac{\varphi}{\delta}) \) for every \( \lambda \in D_F \). Let \( d \) be the smallest rational integer with the property that there exists \( \tilde{\delta} \in D_F \) with \( \tilde{\delta}d = d \). Then \( \xi \) can be written as a ratio \( \xi = \frac{\tilde{\varphi}}{\tilde{\delta}} = \frac{\eta}{\delta} \) where \( \tilde{\delta} \) is a positive integer and \( \eta_0 \in D_F \). For every \( \lambda \in D_F, \Phi_u(\frac{\eta_0 + \lambda\tilde{\delta}}{d}) = \Phi_u(\frac{\eta_0}{d} + \lambda) = \Phi_u(\frac{\eta_0}{d}) \).

Thus, it is not restrictive to consider the integer entries in \( \phi(\eta_0) \) as elements in \( \mathbb{Z}_d \), the residue class ring \( \mathbb{Z}/d\mathbb{Z} \). Moreover, for later use, we have

\[
\Phi_u(\xi) = \Phi_u(\frac{\eta}{\delta}) = \Phi_u(\frac{\eta_0}{d}) = D(u)\phi(\frac{\eta_0}{d}) - \lfloor D(u)\phi(\frac{\eta_0}{d}) \rfloor = \frac{1}{d} \left( D(u)\phi(\eta_0) - d\left\lfloor \frac{D(u)\phi(\eta_0)}{d} \right\rfloor \right). \tag{5}
\]

**Theorem 1.** The set of mappings \( \mathcal{M} = \{\Phi_u \mid u \in \mathcal{U}(F)\} \) is closed under composition. Moreover,

1) \( \Phi_{uv} = \Phi_u \circ \Phi_v, \forall u, v \in \mathcal{U}(F) \), where "\( \circ \)" denotes mapping composition;

2) \( \Phi_1 = \) identity mapping where \( 1 \in \mathcal{U}(F) \) is the unity of \( F \).

3) \( \Phi_{u^{-1}} = \Phi_u^{-1}, \forall u \in \mathcal{U}(F) \).
The set $\mathcal{M}$ is a group isomorphic to $\mathcal{U}(\mathbb{F})$ via the homomorphism
\[ \chi : \mathcal{U}(\mathbb{F}) \rightarrow \mathcal{M} \quad \text{given by} \quad \chi(u) = \Phi_u. \]

Proof. Property P2) is trivial whereas P3) is a consequence of P1) and P2). Hence, it is sufficient to prove P1). Since $u$ and $v$ are units, $D(u)$ and $D(v)$ are integral matrices. Thus,
\[
\Phi_u(\Phi_v(\xi)) = \Phi_u(D(v)\phi(\xi) - [D(v)\phi(\xi)]) = D(u)[D(v)\phi(\xi) - [D(v)\phi(\xi)]] - [D(u)]D(v)\phi(\xi) + D(u)[D(v)\phi(\xi)] = D(u)D(v)\phi(\xi) - [D(u)v\phi(\xi)] = \Phi_{uv}(\xi).
\]
Properties P1), P2), and P3) imply that $\mathcal{M}$ is a group and that $\chi$ is a group isomorphism.

The mappings $\Phi_u \in \mathcal{M}$ partition $\mathbb{T}_n$ into disjoint orbits $\mathcal{C}_u(\xi)$ where $\xi$ is any point in the orbit. Also, $\mathbb{H}_n = \mathbb{R}^n/\mathbb{Z}^n$ is partitioned into orbits of irrational points of $\mathbb{F}$. As it will be shortly established in Theorem 2, these orbits have infinitely many elements and they may have common limit points.

**Lemma 1.** Given two distinct elements $u$ and $v$ in $\mathcal{U}(\mathbb{F})$, if $\Phi_u(\xi) = \Phi_v(\xi)$ then $\xi$ is a rational point, namely, $\xi \in \mathbb{F}$.

Proof. If $\Phi_u(\xi) = \Phi_v(\xi)$ then $(D(u) - D(v))\phi(\xi) = [D(u)\phi(\xi)] - [D(v)\phi(\xi)]$. Since $[D(u)\phi(\xi)]$ and $[D(v)\phi(\xi)]$ are integral vectors and $D(u) - D(v)$ is a non-singular integral matrix, it follows that $\phi(\xi)$ is a point with rational coordinates.

**Corollary 1.** Any finite subset $\mathcal{A} = \{\xi_1, \xi_2, \ldots, \xi_L\} \subset \mathbb{F}$ that is invariant under the action of $\mathcal{U}(\mathbb{F})$ is a subset of $\mathbb{F}$. 

**Lemma 2.** Consider $\xi \in \mathbb{F}$ such that $\phi(\frac{\xi}{\delta}) \in \mathbb{T}_n$ with $\xi$ and $\delta$ relatively prime in $\mathcal{D}_F$. Given a fundamental unit $u \in \mathcal{U}(\mathbb{F})$, there exists a smallest positive integer $t(u)$ such that $\Phi_{u^t(u)}(\frac{\xi}{\delta}) = \phi(\frac{\xi}{\delta})$. Moreover, the set
\[
\left\{ \xi_h \in \mathcal{D}_F : \frac{\xi_h}{\delta} = \Phi_{u^h}(\frac{\xi}{\delta}), \ h = 0, \ldots, t(u) - 1 \right\}
\]
consists of $t(u)$ integers in $\mathbb{F}$, and $d = \delta\tilde{\delta}$ is a factor of $N_\mathbb{F}(u^{t(u)} - 1)$.

Proof. Define $\tilde{\delta}$ and $d$ as in Remark 1. As observed there, $\Phi_v(\frac{\xi + nd\delta}{\delta}) = \Phi_u(\frac{\xi}{\tilde{\delta}})$ for all $v \in \mathcal{U}(\mathbb{F})$, so $\xi$ may be taken from $\mathcal{F}(\delta)$. It follows that the number $t(u)$ of images $\phi(\frac{\xi}{\delta}) \in \mathbb{T}_n$ of elements $\frac{\xi}{\delta} \in \mathbb{F}$ that are distinct is upper bounded by $N_\mathbb{F}(\delta)$. Therefore, $t(u)$ is finite, and we define it as the smallest positive integer such that the vectors
\[
\Phi_{u^h}(\frac{\xi}{\delta}) = \Phi_{\psi}(\frac{\xi}{d}) = \frac{1}{d} \left( D(u^h)\phi(\xi\delta) - D(\frac{1}{d}D(u^h)\phi(\xi\delta)) \right), \ \text{for} \ h = 0, \ldots, t(u) - 1,
\]
are distinct. The rightmost term shows that the $t(u)$ elements $D(u^h)\phi(\xi \delta) \mod d$ are distinct. Since

$$D(u^h)\phi(\xi \delta) \mod d = \phi(u^h \xi \delta) \mod d, \quad h = 0, \ldots, t(u) - 1,$$

the $t(u)$ elements $u^h \xi \delta \mod d$ are distinct, whence the $t(u)$ elements $u^h \xi \mod \delta$ are distinct also. Finally, from $\xi = u^{t(u)} \xi \mod \delta$, it follows that $\delta \mid u^{t(u)} - 1$, and consequently, $d \mid N_F(u^{t(u)} - 1)$. \hfill \square

**Lemma 3.** Let $\xi$ be a rational or irrational point of $\mathbb{F}$. Then for all $\eta$ in the orbit $C_U(\xi)$, one has

$$\text{dist}(\eta, \Omega) = \text{dist}(\xi, \Omega).$$

**Proof.** Since $\eta \in C_U(\xi)$, there is a unit $b \in U(\mathbb{F})$ such that $\eta$ is equal to the dot product $\Phi_b(\xi) \cdot \Omega$. The conclusion is a consequence of the following chain of equalities:

$$\text{dist}(\Phi_b(\xi) \cdot \Omega, \Omega) = \inf_{\theta \in \Omega} |N_F(\Phi_b(\xi) \cdot \Omega - \theta)| = \inf_{\theta \in \Omega} |N_F(D(b)\phi(\xi) \cdot \Omega - [D(b)\phi(\xi)] \cdot \Omega - \theta)|$$

$$= \inf_{\theta' \in \Omega} |N_F(D(b)\phi(\xi) \cdot \Omega - \theta')| = \inf_{\theta' \in \Omega} |\text{det}(D(b))N_F(\xi - D(b)^{-1}\phi(\theta') \cdot \Omega)|$$

$$= \inf_{\theta'' \in \Omega} |N_F(\xi - \theta'')| = \text{dist}(\xi, \Omega).$$

Note that since $\text{det}(D(b)) = \pm 1$, one has $(D(b))^{-1}\phi(\theta') \in \phi(\Omega)$. \hfill \square

**Theorem 2.** If $\xi \in \mathbb{F}$ then:

1) Any orbit $C_U(\xi)$ has finite length.

2) The set of such orbits is a partition of $\mathbb{T}_n$.

If $\xi$ is an irrational point of $\mathbb{F}$ then:

3) Any orbit $C_U(\xi)$ has infinite length.

4) The set of limit points of such orbits is finite, and every limit point is a rational point, that is, it is an element of $\mathbb{F}$. The origin $\phi(0)$ is a possible limit point and it may be common to different orbits.

**Proof.** A rational point $\xi \in \mathbb{H}_n$ can be represented by a vector $\phi(\xi) = \frac{1}{d}z$ with $d$ being the least common multiple of the denominators of the entries in $\phi(\xi)$, written as fractions in reduced form. Hence, $z \in \mathbb{Z}_d^n$. The mappings $\Phi_u$ do not increase $d$, hence $|C_U(\xi)| \leq d^n - 1$. This proves 1).

Suppose two nonzero points $\xi$ and $\eta$ of $\mathbb{F}$ are such that $\xi \notin C_U(\eta)$. If $\Phi_u(\xi) = \Phi_v(\eta)$ for some $u$ and $v$ in $U(\mathbb{F})$, then $\xi = \Phi_{vu^{-1}}(\eta)$, a contradiction. Thus, the orbits are all disjoint and 2) is proved.
The orbit of an irrational point $\xi$ is infinite as a consequence of Lemma 1. This proves 3). Moreover, every point in the orbit is irrational, except possibly its limit points.

To prove 4), some preliminary observations are required: i) Since after the first step every point of the orbit certainly lies in $H_n$, it is not restrictive to assume, for convergence study purposes, that every orbit $C(\xi)$ is contained in $H_n$; ii) the hypercube $H_n$ is a bounded compact set for the Euclidean metric, given that the Euclidean norm $||x||$ of any $x \in H_n$ is upper bounded by $\sqrt{n}$ and lower bounded by zero; iii) the Euclidean norm $||x||$ can be used to study convergence properties of infinite orbits. Therefore, $H_n$ has the Bolzano-Weierstrass property by [11, Theorem B, p.121], that is, any infinite sequence in $H_n$ has a limit point.

As a consequence of these observations, an infinite orbit $C(\xi)$ has at least one limit point in $H_n$. Since by definition a limit point possesses the property that every neighborhood of it contains infinitely many points of the cycle, the set $L$ of limit points is made up of isolated points.

It follows that the cardinality of $L$ is finite. Moreover, $L$ is clearly invariant under the action of $\Phi_u$ for every unit $u$, hence every point in $L$ is in $F$ by Corollary 1.

IV Optimal points

Theorem 2 yields a characterization of optimal points, which is important for theoretical aspects and very useful for computational purposes. The following theorems characterize the nature of optimal points more explicitly, and furnish well-defined methods for computing both an optimal point and the corresponding $M(F)$.

**Theorem 3.** In the algebraic number field $F$ with group of units $\mathbb{U}(F)$ of rank $r \geq 1$, any optimal point is of the form

$$\xi_o = \frac{\eta}{\delta} = \frac{\eta_o}{d} = \frac{\sum_i x_i \omega_i}{d}$$

where $d$ is a positive integer, $x_i \in \mathbb{Z_d}$, $i = 1, \ldots, n$, and $\gcd(d, x_1, \ldots, x_n) = 1$. The numerator $\eta$ and denominator $\delta$ of $\xi_o$ are relatively prime in $\mathfrak{O}_F$. Moreover:

1) $\eta$ is an element of $\mathfrak{S}(\delta)$, the transversal of $\mathfrak{S}(\delta)^* / \psi_{\delta}(\mathbb{U}(F))$, at maximum distance from the $\mathfrak{O}_F$-ideal $\delta \mathfrak{O}_F$.

2) $d$ is a common divisor of $D_1, \ldots, D_r$, where $D_i = N_F(u_i^{N_i} - 1)$, $u_i$ is a fundamental unit of $F$, and $N_i$ is a divisor of $\varphi(d)$ (the Euler totient function) for $i = 1, \ldots, r$. Therefore, $d$ is a divisor of $\gcd\{D_1, \ldots, D_r\}$.

3) The vector $\phi(\eta_o)$ is an eigenvector of the eigenvalue 1 of $D(u_i)^{N_i}$ modulo $d$ for $i = 1, \ldots, r$, that is, $\phi(\eta_o)$ is a common solution of the $r$ homogeneous systems $(D(u_i)^{N_i} - I)\phi(\eta_o) = \phi(0) \bmod d$, where $\phi(0)$ denotes the all-zero vector.

4) Every point in the orbit $C(\xi_o)$ is optimal. Furthermore, $\lcm\{N_1, \ldots, N_r\} \leq |C(\xi_o)| \leq \prod_{i=1}^r N_i$. 
Proof. Theorem 2 shows that $M(F)$ is necessarily rational: If an irrational point is an optimal point, its infinite orbit has a rational limit point that is also optimal. Thus, in any case $\varsigma_0 \in F$.

Again, define $d$ and $\bar{\delta}$ as in Remark 1. The conclusion is a direct consequence of writing the mapping $\Phi_v(\frac{\eta}{\delta})$ for any unit $v$ in the form

$$\Phi_v(\frac{\eta}{\delta}) = D(\delta^{-1}) \left( D(v)\phi(\eta) - D(\delta) \left\lfloor \frac{D(v)\phi(\eta)}{\delta} \right\rfloor \right).$$

This equation shows that since $\eta \in \mathfrak{F}(\delta)^*$, then it can be chosen among the coset leaders $\tau_1, \ldots, \tau_s$ of the subgroup $\mathfrak{F}(\delta)^*/\psi_{\bar{\delta}}(U(F))$ in $\mathfrak{F}(\delta)^*$, where $s = \varphi(\delta)/[\mathfrak{F}(\delta)/\psi_{\bar{\delta}}(U(F))]$. Furthermore, $\eta$ is the coset leader whose distance from the $O/B\times F$-ideal $\delta O/B \times F$ is maximum by the definition of $M(F)$. This proves 1).

Since the orbit of a rational point has finite length, then for every fundamental unit $u_i \in U(F), i = 1, \ldots, r$, an integer $N_i$ exists such that

$$\Phi_{u_i^{N_i}}(\frac{\eta}{\delta}) = \phi(\frac{\eta}{\delta}).$$

Thus, $\delta | (u_i^{N_i} - 1)$ for $i = 1, \ldots, r$. It follows that for each $u_i$, the minimal $N_i$ is the order of the cyclic subgroup of $\mathfrak{F}(\delta)^*$ generated by $u_i$, and all these orders are factors of the exponent of the subgroup $\psi_{\bar{\delta}}(U(F))$ of $\mathfrak{F}(\delta)^*$. This proves 2). [For future reference, note that (7) implies that $D(u_i^{N_i})\phi(\eta_o) - d \left\lfloor \frac{D(u_i^{N_i})\phi(\eta_o)}{d} \right\rfloor = \phi(\eta_o)$, (8)]

where $\eta_o = \eta\bar{\delta}$. Hence, we can rewrite (8) as the homogeneous linear system

$$[D(u_i^{N_i}) - I]\phi(\eta_o) = \phi(0), \quad i = 1, \ldots, r,$$

in $\mathbb{Z}_d$, where $I$ denotes the $n \times n$ identity matrix.]

Equation (9) shows that $\phi(\eta_o)$ is a common eigenvector of $D(u_i^{N_i})$ corresponding to the eigenvalue 1 modulo $d$ for $i = 1, \ldots, r$. This proves 3).

The properties of the orbits of optimal points are straightforward consequences of Theorem 2. The stated lower and upper bounds on the orbit length follow from the sub-orbit length for every unit $u_i, i = 1, \ldots, r$. This proves 4).

An important open question left by Theorem 3 is the explicit computation of the exponents $N_i$ and, more importantly, the denominator $d$ which is crucial in finding the optimal point. This computational problem has a complete solution for normal fields as it will be shown by the next theorem.

**Theorem 4.** Let $F$ be a normal $n$-degree extension of $\mathbb{Q}$ with automorphism group $\text{Gal}(F/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$, where $\sigma_1$ is the identity mapping. Let $d = \delta\bar{\delta}$ be a rational integer as specified
in Theorem 3, where \( \delta \in \mathcal{O}_F \). Then \( d \) is a common divisor of the norms \( N_F(\sigma_h(u) - \sigma_k(u)) \) where \( u \) is a unit and \( k, h \in \{1, \ldots, n\} \) with \( k \neq h \). In particular, \( d \) is a divisor of the greatest common divisor of the discriminants of the minimal polynomials of the fundamental units.

**Proof.** Equation (9) shows that an optimal point \( \xi_o = \frac{n}{\delta} = \frac{n}{d} \), with \( \eta \) relatively prime to \( \delta \), and \( \eta_o = \eta \delta \), is identified by a common eigenvector of eigenvalue 1 of the matrices \( D(u)^{t(u)} \) modulo \( d \), where \( u \) is any unit and \( t(u) \) is the minimum integer such that \( u^{t(u)} = 1 \mod \delta \). Equation (9) implies that for every unit \( u \), \( (D(u) - aI)\phi(\eta_o) = \phi(0) \mod \delta \), where \( a \) is a \( t(u) \)th root of the unity modulo \( \delta \). Since the entries of \( D(u) \) and \( \phi(\eta_o) \) belong to \( \mathbb{Z}_d \), it follows that \( a \in \mathbb{Z}_d \). The last equation can be conveniently rewritten as

\[
(D(u) - aI)D(\delta)\phi(\eta) = \phi(0) \mod \delta \delta.
\] (10)

Let \( d = \prod_j p_j^{n_j} \) be the rational prime power factorization of \( d \). Let \( \pi_j \) be a prime above \( p_j \) in \( \mathbb{F} \) with inertia index \( f_j \) and ramification index \( e_j \). Hence, we have the factorizations \( \delta = \prod_j \pi_j^{n_j} \) and \( \delta = \prod_j \bar{\pi}_j^{n_j} \), with \( d = \delta \delta \). We can now solve the set of equations

\[
(D(u) - aI)D(\pi_j^{n_j})\phi(\eta) = \phi(0) \mod \pi_j^{n_j} \bar{\pi}_j^{n_j} \quad \forall \ j,
\] (11)

and recover a solution of (10) by the Chinese remainder theorem. Now we consider separately primes \( p_j \) that ramify, are inert, or split in \( \mathcal{O}_F \).

**\( p_j \) ramifies:** Equation (11) is equivalent to

\[
D(\pi_j^{n_j(e_j-1)})[D(u) - aI]\phi(\eta) = \phi(0) \mod \pi_j^{e_j n_j},
\]

which implies \( [D(u) - aI]\phi(\eta) = \phi(0) \mod \pi_j^{n_j} \). Since all the entries in this equation, except the modulus, are in \( \mathbb{Q} \), we obtain a conjugated equation

\[
[D(u) - aI]\phi(\eta) = \phi(0) \mod \sigma(\pi_j^{n_j})
\] (12)

for each automorphism \( \sigma \in \text{Gal}(\mathbb{F}/\mathbb{Q}) \). In \( \mathbb{F} \), equation (12) reads \( (u - a)\eta = 0 \mod \sigma(\pi_j^{n_j}) \). Since \( \eta \) is relatively prime with \( \pi_j \), it can be disregarded, and taking the inverse automorphism we have a set of \( n \) equations \( \sigma^{-1}(u) - a = 0 \mod \pi_j^{n_j} \) because \( \sigma(a) = a \). By considering the difference of any two equations, it follows that \( \pi_j^{n_j} \) is a divisor of \( \sigma_h(u) - \sigma_k(u) \) for every \( h \neq k \). It turns out that \( \pi_j^{n_j} \), and thus \( p_j^{n_j} \), is a divisor of the discriminant of the minimal polynomial of \( u \).

**\( p_j \) is inert:** Equation (11) is equivalent to

\[
[D(u) - aI]\phi(\eta) = \phi(0) \mod p_j^{n_j}.
\] (13)

In \( \mathbb{F} \), equation (13) reads \( (u - a)\eta = 0 \mod p_j^{n_j} \). By applying the Galois automorphisms to it, we obtain a set of \( n \) equations \( \sigma(u) - a = 0 \mod p_j^{n_j} \), because \( \sigma(a) = a \) and \( \sigma(p_j) = p_j \). By considering the difference of any two equations, it follows that \( p_j^{n_j} \) is a divisor of \( \sigma_h(u) - \sigma_k(u) \) for every \( h \neq k \). It turns out that \( p_j^{n_j} \), is a divisor of the discriminant of the minimal polynomial of \( u \).
Corollary 2. Let $\mathbb{F} = \mathbb{Q}(\sqrt{\Delta})$ be a real quadratic field with Galois group $\text{Gal}(\mathbb{F}/\mathbb{Q}) = \{e, \sigma\}$. Let $d = \delta \delta$ be a rational integer as specified in Theorem 3, with $\delta$ an integer in $\mathcal{O}_\mathbb{F}$. Let $u$ be a fundamental unit of norm $\epsilon = \pm 1$. Then $d$ is a divisor of $N_\mathbb{F}(u^2 - \epsilon) = \det(D(u)^2 - \epsilon I)$. If $u$ is written as $u = a_0 + a_1 \sqrt{\Delta}$, where $\Delta$ is the field discriminant, then $d$ is a divisor of $2a_1^2 \Delta$.

V Numerical Results and Conclusions

We proved that the norm-Euclidean minimum $M(\mathbb{F})$ of any number field $\mathbb{F}$ is a rational number $\frac{a}{d}$, where $d$ can be found within a known, finite set of values. Furthermore, a point $\varsigma_0 \in \mathbb{F}$ exists such that $M(\mathbb{F}) = N(\varsigma_0)$. In numerical computations, it is useful to have general upper and a lower bounds on $M(\mathbb{F})$, which are not necessarily the best bounds, but in their generality they are useful for checking the numerical results, and might be useful for theoretical considerations. A lower bound is given by the following
Theorem 5. Let $\pi_m$ be the minimum norm ideal in $\mathcal{O}_F$, then

$$M(F) \geq \frac{1}{N_F(\pi_m)} \geq \frac{1}{2^a} \geq \frac{1}{2^n}, 1 \leq a \leq n.$$ 

Proof. Take $d = N(\pi_m)$, and $\xi_o = d/\pi_m$, therefore the norm of the point $\phi(\xi_o)/d$ is lower bounded by $\frac{1}{N_F(\pi_m)}$. The smallest bound occurs when 2 is prime in $\mathcal{O}_F$. If 2 splits with a factor of minimum inertia degree $f$, then $1/2^f$ is a lower bound.

In conclusion, for $M(F)$ in any algebraic field of degree $n$, we have the bounds $\frac{1}{2^n} \leq M(F) \leq |\Delta|$, where $\Delta$ is the field discriminant which yields the upper bound as shown in [1]. Finally, the computation of $M(F)$, as a consequence of Theorems 3 and 4, and well known results [7], are conveniently summarized as:

**Rank $r = 0$:** These fields are the complex fields $\mathbb{Q}(\sqrt{m})$ of degree 2, with $m$ a negative squarefree integer. The problem was already solved [7], and the Euclidean minimum $M(\mathbb{Q}(\sqrt{m}))$ is

$$M(\mathbb{Q}(\sqrt{m})) = \begin{cases} \frac{|m|+1}{4} & \text{if } \Delta = 4m, \text{ and } m \equiv 2, 3 \mod 4 \\ \frac{(|m|+1)^2}{16|m|} & \text{if } \Delta = m, \text{ and } m \equiv 1 \mod 4 \end{cases}$$

where $\Delta$ is the field discriminant.

**Rank $r = 1$:** These fields are the real fields of degree 2, the mixed (or complex) fields of degree 3, and the totally complex fields of degree 4. The problem was solved by van der Linden, who showed that $M(F)$ is a rational number [12, 13]. If $F$ is totally complex, then the group of units is $E(F) \times U(F)$ where $E(F)$ is a cyclic group of order less than or equal to 12 [10, Table (4.4), p. 345]. Otherwise, $U(F) \cong \mathbb{Z}$ and $E(F) = \{1, -1\}$ [10, Lemma 4.1, p. 343]. Moreover, if $E(F) \neq \{-1, 1\}$, then $d$ is also a divisor of the discriminant of the cyclotomic polynomial $\Phi_N(x)$, where $N$ is a divisor of $|E(F)|$. In the quadratic fields $\mathbb{Q}(\sqrt{m})$, the search for $d$ is restricted to the divisors of $4b^2m$, where $b$ is obtained from a fundamental unit $u = a + b\sqrt{m}$.

**Rank $r \geq 2$:** These are all the fields not included in the previous cases. The problem of computing $d$ is set in context by Theorem 3. By Theorem 4, the search for $d$ is nicely restricted when $F$ is a normal extension of $\mathbb{Q}$.

The numerical results shown in Table 1 are either new or a confirmation that known lower bounds are the actual values of $M(F)$. They have been obtained with MAPLE assuming known integral basis, fundamental units, and torsion generator units, which have been computed using KANT [4].

References

Computation of the norm-Euclidean minimum


Received: November, 2008
<table>
<thead>
<tr>
<th>$p(X)$</th>
<th>$\Delta$</th>
<th>$u(F)$</th>
<th>$r$</th>
<th>$G_{\text{aut}}, G_p$</th>
<th>$Q(\omega)$</th>
<th>$M(K)$</th>
<th>$\phi(\varsigma)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quadratic fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$1, -1, -25$</td>
<td>101</td>
<td>$9 + 2\rho$</td>
<td>1</td>
<td>$C_2, C_2$</td>
<td>--</td>
<td>$\frac{5}{2}$</td>
<td>$(5,1)$</td>
</tr>
<tr>
<td>$1, 0, -102$</td>
<td>102</td>
<td>$101 + 10\rho$</td>
<td>1</td>
<td>$C_2, C_2$</td>
<td>--</td>
<td>$\frac{19}{4}$</td>
<td>$(11,1)$</td>
</tr>
<tr>
<td>$1, 0, -103$</td>
<td>103</td>
<td>$227528 + 22419\rho$</td>
<td>1</td>
<td>$C_2, C_2$</td>
<td>--</td>
<td>$\frac{279}{103}$</td>
<td>$(412,37)$</td>
</tr>
<tr>
<td>$1, -1, -26$</td>
<td>105</td>
<td>$37 + 8\rho$</td>
<td>1</td>
<td>$C_2, C_2$</td>
<td>--</td>
<td>$\frac{1}{2}$</td>
<td>$(60,39)$</td>
</tr>
<tr>
<td>Cubic fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$1, -1, -10, 13$</td>
<td>1929</td>
<td>$-3 + \rho, 5 - 5\rho + \rho^2$</td>
<td>2</td>
<td>$C_1, S_3$</td>
<td>--</td>
<td>1</td>
<td>$(83, -12, -11)$</td>
</tr>
<tr>
<td>$1, -1, -34, 61$</td>
<td>103$^2$</td>
<td>$\frac{79}{6} - 19\rho + \frac{3}{2}\rho^2$</td>
<td>2</td>
<td>$C_3, C_3$</td>
<td>--</td>
<td>$\frac{93}{103}$</td>
<td>$(1324, -837, 71)$</td>
</tr>
<tr>
<td>$1, -1, -36, -4$</td>
<td>109$^2$</td>
<td>$-13 + 5\rho + \rho^2$</td>
<td>2</td>
<td>$C_3, C_3$</td>
<td>--</td>
<td>$\frac{76}{109}$</td>
<td>$(1034, -127, 11)$</td>
</tr>
<tr>
<td>$1, -1, -42, -80$</td>
<td>127$^2$</td>
<td>$781 + 93\rho - 25\rho^2$</td>
<td>2</td>
<td>$C_3, C_3$</td>
<td>--</td>
<td>$\frac{94}{127}$</td>
<td>$(808, 59, -26)$</td>
</tr>
<tr>
<td>$1, -1, -52, -64$</td>
<td>157$^2$</td>
<td>$1495 + 965\rho - 139\rho^2 - 523 - \frac{977}{4}\rho - \frac{135}{2}\rho^2$</td>
<td>2</td>
<td>$C_3, C_3$</td>
<td>--</td>
<td>$\frac{118}{157}$</td>
<td>$(-313, 6, 9)$</td>
</tr>
<tr>
<td>Quartic fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$1, 1, -3, -1, 1$</td>
<td>725</td>
<td>$\rho, -1 + \rho, 1 + \rho$</td>
<td>3</td>
<td>$C_2, D_8$</td>
<td>$\omega_5$</td>
<td>$\frac{6}{11}$</td>
<td>$(-17, -4, 48, 30)$</td>
</tr>
<tr>
<td>$1, 1, 0, -2, -1$</td>
<td>-275</td>
<td>$\rho, 1 + \rho$</td>
<td>2</td>
<td>$C_2, D_8$</td>
<td>$\omega_5$</td>
<td>$\frac{1}{5}$</td>
<td>$(7, 11, -7, -6)$</td>
</tr>
<tr>
<td>$1, 0, 2, 3, 1$</td>
<td>117</td>
<td>$1 + 3\rho - \rho^2 + \rho^3$</td>
<td>1</td>
<td>$C_2, D_8$</td>
<td>$\varsigma_3$</td>
<td>$\frac{1}{7}$</td>
<td>$(2, 3, 3, 6, 3)$</td>
</tr>
<tr>
<td>$1, 1, 1, 1, 1$</td>
<td>125</td>
<td>$1 + \rho$</td>
<td>1</td>
<td>$C_4, C_4$</td>
<td>$\omega_5$</td>
<td>$\frac{1}{3}$</td>
<td>$(14, 3, 7, 11)$</td>
</tr>
<tr>
<td>$1, 2, 0, -1, 1$</td>
<td>189</td>
<td>$\rho$</td>
<td>1</td>
<td>$C_2, D_8$</td>
<td>$\varsigma_3$</td>
<td>$\frac{1}{3}$</td>
<td>$(7, 6, 3, -1)$</td>
</tr>
<tr>
<td>$1, 0, 0, 1, 1$</td>
<td>229</td>
<td>$\rho$</td>
<td>1</td>
<td>$C_1, S_4$</td>
<td>--</td>
<td>$\frac{1}{3}$</td>
<td>$(1, 2, 2, 3)$</td>
</tr>
<tr>
<td>$1, 0, 1, 1, 1$</td>
<td>257</td>
<td>$\rho$</td>
<td>1</td>
<td>$C_1, S_4$</td>
<td>--</td>
<td>$\frac{1}{3}$</td>
<td>$(1, 0, 1, 1)$</td>
</tr>
<tr>
<td>Quintic fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$1, 1, -4, -3, 3, 1$</td>
<td>14641</td>
<td>$\rho, 1 - \rho$</td>
<td>4</td>
<td>$C_5, C_5$</td>
<td>--</td>
<td>$\frac{1}{11}$</td>
<td>$(20, 4, -14, 1, 4)$</td>
</tr>
</tbody>
</table>

**Column labels:**

$p(X)$: polynomial defining $F$ | $\Delta$: discriminant of $F$ | $\rho$: root of $p(X)$

$u(F)$: fundamental units | $r$: rank of the unit group | $G_p$: Galois group of $p(X)$

$G_{\text{aut}}$: Automorphism group of $F$ | $Q(\omega)$: quadratic subfields of $F$ | $M(F)$: norm-Euclidean minimum

$\phi(\varsigma)$: 0-optimal point in power basis

$\varsigma$: root of $x^2 + x + 1$, $\omega_5$: root of $x^2 - x - 1$,

$C_j$: cyclic group of order $j$, $D_8$: dihedral group of order 8, $S_n$: symmetric group on $n$ letters.

Table 1: Norm-Euclidean minima of algebraic number fields