

ON SOLVING RELATIVE NORM EQUATIONS IN ALGEBRAIC NUMBER FIELDS

C. FIEKER, A. JURK, AND M. POHST

ABSTRACT. Let $\mathbb{Q} \subseteq \mathcal{E} \subseteq \mathcal{F}$ be algebraic number fields and $M \subset \mathcal{F}$ a free $o_{\mathcal{E}}$ -module. We prove a theorem which enables us to determine whether a given relative norm equation of the form $|N_{\mathcal{F}/\mathcal{E}}(\eta)| = |\theta|$ has any solutions $\eta \in M$ at all and, if so, to compute a complete set of nonassociate solutions. Finally we formulate an algorithm using this theorem, consider its algebraic complexity and give some examples.

1. INTRODUCTION

Solving norm equations is a central problem in the area of algebraic number theory. Although there is an algorithm for solving absolute norm equations (e.g. see [1] or [8, §§5.3, 6.4]), none (except the absolute one) exists in the relative case. We outline a new algorithm to decide whether a relative norm equation has solutions at all and then, if there are solutions to compute a complete set of nonassociate (with respect to units of relative norm 1) solutions. Finally we discuss the complexity of this algorithm and give some examples.

2. PRELIMINARIES

First, we introduce several definitions and notations. We consider the following situation:

$\begin{array}{c} \mathcal{F} = \mathcal{E}(\beta) \\ \Bigg/ \quad n \\ \mathcal{E} = \mathbb{Q}(\alpha) \\ \Bigg/ \quad m \\ \mathbb{Q} \end{array}$	<p>Let $\alpha = \alpha^{(1)}, \dots, \alpha^{(m)}$ be the roots of the monic irreducible polynomial $f \in \mathbb{Q}[t]$, $\mathcal{E} := \mathbb{Q}(\alpha)$. Furthermore, let β be a root of a monic irreducible polynomial $g \in \mathcal{E}[t]$ and $\mathcal{F} := \mathcal{E}(\beta)$. We assume that $\alpha^{(1)}, \dots, \alpha^{(m_1)}$ denote the real roots of f and that $\alpha^{(m_1+1)} = \overline{\alpha^{(m_1+m_2+1)}}$, \dots, $\alpha^{(m_1+m_2)} = \overline{\alpha^{(m_1+2m_2)}}$ are in $\mathbb{C} \setminus \mathbb{R}$. For an arbitrary $\eta \in \mathcal{E}$ we define $\eta^{(i)}$ ($1 \leq i \leq m$) as the image of η under the \mathbb{Q}-isomorphism from \mathcal{E} to $\mathcal{E}^{(i)} := \mathbb{Q}(\alpha^{(i)})$ which maps α to $\alpha^{(i)}$. The norm of an element η of \mathcal{E} is defined in the usual way: $N(\eta) := N_{\mathcal{E}/\mathbb{Q}}(\eta) := \prod_{i=1}^m \eta^{(i)}$. The definitions for \mathcal{F} are essentially the same, but here we have to be careful about which field we are using as base field. In general, the conjugates cannot be ordered in real and pairs of complex ones and — of course — we get different conjugates</p>
---	---

Received by the editor August 30, 1994 and, in revised form, March 27, 1995 and July 20, 1995.

1991 *Mathematics Subject Classification.* Primary 11Y40.

Key words and phrases. Algebraic number theory, norm equations, relative norm equations, relative extensions.

when we consider \mathcal{F} as an extension of \mathcal{E} rather than as an extension of \mathbb{Q} . We will discuss this in detail later.

The ring of integers of a field \mathcal{K} is denoted by $\mathfrak{o}_{\mathcal{K}}$ in the sequel.

3. ABSOLUTE NORM EQUATIONS

In this section we give a short review on the Fincke–Pohst algorithm to solve absolute norm equations.

Given an arbitrary, but fixed $k \in \mathbb{Z}_{>0}$ and $M \subset \mathcal{E}$ a free \mathbb{Z} module of \mathcal{E} , we want to find all $\eta \in M$ subject to

$$(3.1) \quad N(\eta) = k$$

or

$$(3.2) \quad |N(\eta)| = k,$$

i.e., we want to determine if solutions exist and, if so, compute all of them.

If M is of full rank m , we fix a maximal system of independent units $\epsilon_1, \dots, \epsilon_r$ ($r = m_1 + m_2 - 1$) of its ring of multipliers. For practical computations it is advisable to use LLL-reduction in the logarithmic lattice to produce units for which the absolute values of each of their conjugates are close to 1. The next lemma gives explicit bounds for a complete set of nonassociate solutions.

Lemma 3.1. *Let η be a solution of (3.2). Then there exists a unit ϵ and a solution $\tilde{\eta} = \eta\epsilon$ subject to*

$$(3.3) \quad \frac{1}{R_i} \leq \frac{|\tilde{\eta}^{(i)}|}{\sqrt[m]{k}} \leq R_i \quad (1 \leq i \leq m),$$

where

$$R_i := \exp \left(\frac{1}{2} \sum_{j=1}^{m_1+m_2-1} |\log(|\epsilon_j^{(i)}|)| \right).$$

Proof. See [1, (6.3) Lemma] or [8, Theorem (4.2), Chapter 6]. \square

If M is not of rank m , then it is not known how to compute realistic bounds on the conjugates of the (finitely many) solutions of (3.2). Hence, in that case we need to stipulate bounds R_i such that any solution $\tilde{\eta}$ satisfies (3.3). This works well if we are only interested in “small solutions”, say with coefficients bounded by 10^6 .

Furthermore, we need the following, rather technical, lemma from [1, (6.23) Satz] or [8, Theorem (3.8), Chapter 5]:

Lemma 3.2. *For arbitrary $\gamma, r \in \mathbb{R}_{>0}$ define the functions $h : \mathbb{R}_{>1} \rightarrow \mathbb{R} : t \mapsto \frac{t}{t-1} - \frac{1}{\log t}$ and $g : \mathbb{R}_{>1} \rightarrow \mathbb{R} : t \mapsto (1 - h(t))t^{h(t)} + h(t)t^{h(t)-1}$. Then there exists a unique zero $\lambda = \lambda(\gamma, r)$ of $g(t) - (1 + \frac{\gamma}{r})^{2/m}$.*

Using the previous two lemmas, one can prove the following theorem, which will allow us to solve absolute norm equations of the type (3.2) or (3.1).

Theorem 3.3. *For arbitrary $\gamma \in \mathbb{R}_{>0}$ let $\lambda = \lambda(\gamma, k)$ as in Lemma 3.2. Define constants $L_i := \lfloor \frac{-2 \log R_i}{\log \lambda} \rfloor$, $U_i := \lceil \frac{2 \log R_i}{\log \lambda} \rceil$ ($1 \leq i \leq m$) with R_i as in Lemma 3.1.*

If (3.2) is solvable, then there exists $\mathbf{r} = (r_1, \dots, r_m) \in \mathbb{Z}^m$ and a solution η of (3.2) subject to (3.3), and

$$(3.4) \quad \sum_{j=1}^m \lambda^{r_j} |\eta^{(j)}|^2 \leq m(k + \gamma)^{2/m}.$$

The coordinates of \mathbf{r} satisfy $\sum_{j=1}^m r_j = 0$, $L_j \leq r_j \leq U_j$ ($1 \leq j \leq m$) and $r_{m_1+j} = r_{m_1+m_2+j}$ for all $1 \leq j \leq m_2$ with at most one exception, where we have $r_{m_1+j} + 1 = r_{m_1+m_2+j}$. For rank $M = m$, any solution of (3.2) is associate with one satisfying (3.4).

Remark 3.4. Representing η in a basis of M , the left-hand side of (3.4) becomes a positive definite quadratic form over M , so that the solutions of the inequality are lattice points inside an ellipsoid.

The basic idea in the proof of the theorem above is an observation due to M. Pohst which guarantees (under certain conditions) the existence of some vector $\lambda \in \mathbb{R}_{>0}^m$ with $\sum_{j=1}^m \lambda_j |\eta^{(j)}|^2 = mk$ for every solution η of (3.2). The main task in the proof then is to obtain a finite set of candidates for the λ 's. This was achieved by U. Fincke [1] who transformed our problem into a discrete one by considering only vectors of the form $(\lambda^{r_1}, \dots, \lambda^{r_m})$, $r_j \in \mathbb{Z}$. In the next step, we obtain bounds for the r_j 's from the bounds for the solutions. Finally, we reduce the set of the admissible exponent vectors $\mathbf{r} = (r_1, \dots, r_m)$.

To use this theorem for solving (3.2), one has to calculate the set of all admissible $\mathbf{r} \in \mathbb{Z}^m$, for each such \mathbf{r} to compute the set of all $\eta \in M$ subject to (3.4) and, finally, to determine the solutions of (3.2) among them.

The following statement concerns the algebraic complexity when using the Fincke-Pohst method to enumerate the points of the ellipsoids.

Theorem 3.5. *Let $k \in \mathbb{Z}$ and the signature (m_1, m_2) be fixed. Then there exists a $v > 1$ depending only on the conjugates of a \mathbb{Z} basis of M and a sufficiently large $U \geq \max_{j=1}^m U_j$, U_j as in Theorem 3.3, such that the number of arithmetic operations (addition, multiplication, division, calculation of square roots) used to solve (3.2) with the algorithm described above is bounded by*

$$(m_2 + 1) \left(3 - \frac{4 \log k}{m \log \lambda} + \frac{4 \log U}{\log \lambda} \right)^{m_1 + m_2 - 1} (2Um^{2/3}v\lambda^{1/2} \left(1 + \frac{\lambda}{k} \right)^{1/m})^{m/2} (2m^3 + 24m^2).$$

Proof. See [1, (7.5) Satz]. □

4. RELATIVE NORM EQUATIONS

Before we sketch the theory and the algorithm, we make some further definitions. Let $M \subset \mathcal{F}$ be a free $o_{\mathcal{E}}$ -module. As above, we assume the rank of M to be n in order to produce bounds. For an arbitrary $\theta \in o_{\mathcal{E}}$ we want to decide if there are any $\eta \in M$ satisfying

$$(4.1) \quad N_{\mathcal{F}/\mathcal{E}}(\eta) = \theta$$

or

$$(4.2) \quad |N_{\mathcal{F}/\mathcal{E}}(\eta)| = |\theta|$$

and, if so, we will compute a complete set of nonassociate solutions.

Although the algorithm described in the previous section could, in principle, be used to accomplish this (certainly one can solve $N(\eta) = N_{\mathcal{E}/\mathbb{Q}}(N_{\mathcal{F}/\mathcal{E}}(\eta)) =$

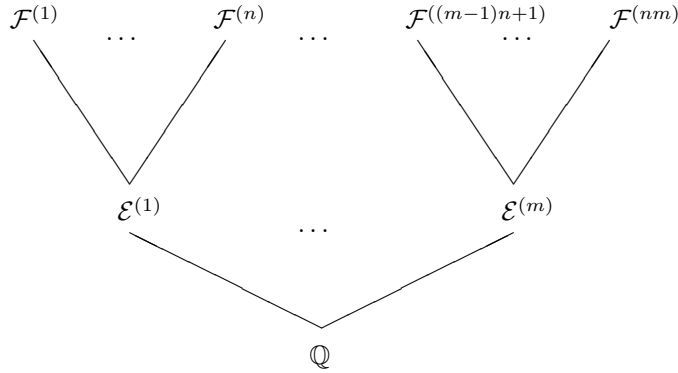


FIGURE 1. The ordering of the conjugate fields

$N_{\mathcal{E}/\mathbb{Q}}(\theta)$ and then test the solutions), it turns out to be far too expensive in terms of computation time. Hence, the approach for the absolute case needs to be changed appropriately.

To deal with the difficulties concerning the conjugates of \mathcal{F} arising from the fact that we can consider \mathcal{F} both as an extension of \mathcal{E} and of \mathbb{Q} , we fix the ordering of the conjugate fields as described in Figure 1. To simplify notation, we define the following abbreviation: $N_{\mathcal{F}/\mathcal{E}}^{(j)}(\gamma) := N_{\mathcal{F}^{((j-1)n+1)}/\mathcal{E}^{(j)}}(\gamma^{((j-1)n)}) = \prod_{i=1}^n \gamma^{((j-1)n+i)}$. We require that the conjugate fields $\mathcal{E}^{(1)}, \dots, \mathcal{E}^{(m)}$ of \mathcal{E} are ordered as described in §2.

For the real conjugate fields $\mathcal{E}^{(i)}$ ($1 \leq i \leq m_1$) we stipulate furthermore that the conjugate fields of \mathcal{F} , which are extensions of these, are ordered in a similar manner. For $1 \leq i \leq m_1$ we require that $\mathcal{F}^{((i-1)n+j)} \subseteq \mathbb{R}$ ($1 \leq j \leq s_i$) and $\mathcal{F}^{((i-1)n+s_i+j)} = \overline{\mathcal{F}^{((i-1)n+s_i+t_i+j)}} \not\subseteq \mathbb{R}$ ($1 \leq j \leq t_i$), $s_i + 2t_i = n$, where (s_i, t_i) denotes the relative signature of $\mathcal{F}^{((i-1)n+1)}$ over $\mathcal{E}^{(i)}$ [4, Lemmas 3.1–3.4].

As in the absolute case, the first task is to obtain bounds for a set containing all non-associate solutions of (4.2) or (4.1). In the previous section we used units of the ring of multipliers of M to transform arbitrary solutions to those contained in a bounded region. In order to preserve (4.1), one has to use units ϵ where $N_{\mathcal{F}/\mathcal{E}}(\epsilon) = 1$, whereas for (4.2), it suffices to require that $N_{\mathcal{F}/\mathcal{E}}(\epsilon)$ is a torsion unit of \mathcal{E} . Here we will restrict ourselves to units of the form $\epsilon^n / N_{\mathcal{F}/\mathcal{E}}(\epsilon)$. Clearly, we have $N_{\mathcal{F}/\mathcal{E}}(\epsilon^n / N_{\mathcal{F}/\mathcal{E}}(\epsilon)) = N_{\mathcal{F}/\mathcal{E}}(\epsilon^n) / N_{\mathcal{F}/\mathcal{E}}(\epsilon)^n = 1$. Let $\epsilon_1, \dots, \epsilon_r$ be a maximal system of independent units of the ring of multipliers of M . We have the following lemma, which corresponds to Lemma 3.1:

Lemma 4.1. *Let η be a solution of (4.2) or (4.1). Then there exists a unit ϵ and a solution $\tilde{\eta} = \eta\epsilon$ of (4.2) and (4.1) subject to*

$$(4.3) \quad \frac{1}{R_{(j-1)n+i}} \leq \frac{|\tilde{\eta}^{((j-1)n+i)}|}{\sqrt[n]{|\theta^{(j)}|}} \leq R_{(j-1)n+i} \quad (1 \leq i \leq m, 1 \leq j \leq n),$$

where

$$R_{(j-1)n+i} = \exp \left(\frac{n}{2} \sum_{l=1}^r |\log(|\epsilon_l^{((j-1)n+i)}|)| + \frac{1}{2} \sum_{l=1}^r |\log(|N_{\mathcal{F}/\mathcal{E}}^{(j)}(\epsilon_l)|)| \right).$$

Proof. The proof is essentially the same as in the absolute case. The bounds are worse than those in Lemma 3.1 because of the restricted set of units used for the transformation [4, Lemma 4.1]. \square

Assuming that we have bounds for the conjugates of solutions from a different source, we can again generalize the method to modules M of rank less than n , as in the last section.

We note that the bounds here are not a generalization of those obtained in Lemma 3.1. Having established this lemma, and using Lemma 3.2 of the preceding section, we obtain the following theorem:

Theorem 4.2. *For arbitrary $\gamma_j \in \mathbb{R}_{>0}$ let $\lambda_j = \lambda(\gamma_j, |\theta^{(j)}|)$ ($1 \leq j \leq m$) as in Lemma 3.2. Define constants $L_i^{(j)} := \lfloor \frac{-2 \log R_{(j-1)n+i}}{\log \lambda_j} \rfloor$, $U_i^{(j)} := \lceil \frac{2 \log R_{(j-1)n+i}}{\log \lambda_j} \rceil$ ($1 \leq i \leq n$) with $R_{(j-1)n+i}$ as in Lemma 4.1. Then for every solution ν of (4.1) there exists a unit ϵ with $N_{\mathcal{F}/\mathcal{E}}(\epsilon) = 1$, $r^{(j)} = (r_1^{(j)}, \dots, r_n^{(j)}) \in \mathbb{Z}^n$ ($1 \leq j \leq m$) and a solution $\eta = \epsilon\nu$ of (4.1) subject to (4.3) such that*

- (1) $\sum_{i=1}^n \lambda_j^{r_i^{(j)}} |\eta^{((j-1)n+i)}|^2 \leq n(|\theta^{(j)}| + \gamma_j)^{2/n}$, $1 \leq j \leq m$;
- (2) $\sum_{i=1}^m r_i^{(j)} = 0$, $1 \leq j \leq m$;
- (3) $L_i^{(j)} \leq r_i^{(j)} \leq U_i^{(j)}$, $1 \leq i \leq n$, $1 \leq j \leq m$;
- (4) For $1 \leq j \leq m_1$ we have in addition $r_{s_j+i}^{(j)} = r_{s_j+t_j+i}^{(j)}$ for all $1 \leq i \leq t_j$ with at most one exception, where we have $r_{s_j+i}^{(j)} + 1 = r_{s_j+t_j+i}^{(j)}$.

Proof. Let ϵ and $\eta = \tilde{\nu}$ be as in Lemma 4.1. For $1 \leq j \leq m$ and $1 \leq i \leq n$ define $y_i^{(j)} := |\theta^{(j)}|^{-2/n} |\eta^{((j-1)n+i)}|^2$. Clearly, $\prod_{i=1}^m y_i^{(j)} = 1$. Since $y_i^{(j)}$ and λ_j are positive, we can find $\tilde{r}_i^{(j)} \in \mathbb{Z}$, $\tilde{e}_i^{(j)} \in [0, 1)$ with

$$(4.4) \quad y_i^{(j)} = \lambda_j^{-\tilde{r}_i^{(j)} + \tilde{e}_i^{(j)}}$$

and $0 = \sum_{l=1}^n \tilde{r}_l^{(j)} = \sum_{l=1}^n \tilde{e}_l^{(j)}$. By performing some lengthy computations, we can change the \tilde{e} 's and the \tilde{r} 's to fulfill conditions (2) and (4) and then verify (3) using (4.4). As in the absolute case, the validity of (1) is a consequence of Lemma 3.2 [4, Satz 4.4]. \square

A straightforward computation gives $|N_{\mathcal{F}/\mathcal{E}}^{(j)}(\eta)| \leq |\theta^{(j)}| + \gamma_j$ for all η satisfying (1) of Theorem 4.2.

Analogous to the description given in the paragraph after Remark 3.4, we get an algorithm for solving (4.2). We note that the inequalities (1) describe ellipsoids defined via the positive definite quadratic forms [4, Lemma 4.6]

$$x = (x_1, \dots, x_n) \mapsto \sum_{i=1}^n \lambda_j^{r_i^{(j)}} |x_j|^2 \quad (1 \leq j \leq m).$$

Their lattice points can be calculated with a modified Fincke-Pohst enumeration algorithm.

5. A MODIFIED FINCKE-POHST ALGORITHM

A main part in solving norm equations is the enumeration of all points in suitable ellipsoids. In this section we present a modification of the Fincke-Pohst method

adopted to relative norm equations. We consider the following situation: Let $A^{(i)} \in \mathbb{C}^{n \times n}$ be positive definite, $C^{(i)} > 0$ subject to $A^{(i)} = \overline{A}^{(i+m_2)}$, $C^{(i)} = C^{(i+m_2)}$ ($m_1 < i \leq m_1 + m_2$). We present an algorithm to calculate all $x \in M$ subject to

$$\overline{x}_{(i)}^{\text{tr}} A^{(i)} x_{(i)} \leq C^{(i)},$$

where $x_{(i)} = (x^{((i-1)n+1)}, \dots, x^{((i-1)n+n)})^{\text{tr}}$. Let ν_1, \dots, ν_n be an $\mathcal{O}_{\mathcal{E}}$ -basis of M . For $x \in M$ we have $x = \sum_{l=1}^n z_l \nu_l$ with $z_i \in \mathcal{O}_{\mathcal{E}}$ and $x^{((i-1)n+j)} = \sum_{l=1}^n z_l^{(i)} \nu_l^{((i-1)n+j)}$. Defining $V_i := (\nu_l^{((i-1)n+j)})_{\substack{1 \leq j \leq n \\ 1 \leq l \leq n}}$, we set

$$Q_i(x) := \overline{x}_{(i)}^{\text{tr}} A^{(i)} x_{(i)} = (z_1, \dots, z_n) \overline{V}_i^{\text{tr}} A^{(i)} V_i (z_1, \dots, z_n)^{\text{tr}}.$$

Let $B_i := \overline{V}_i^{\text{tr}} A^{(i)} V_i$. Using the algorithm for quadratic supplement (see [3, (2.3)]), we obtain $\underline{z}^{\text{tr}} B_i \underline{z} = \sum_{l=1}^n q_{l,l}^{(i)} |z_l^{(i)}|^2 + \sum_{s=l+1}^n q_{l,s}^{(i)} z_s^{(i)} |z_l^{(i)}|^2$. (Note that we have $q_{l,l}^{(i)} > 0$ since B_i is positive definite.) This yields the following straightforward algorithm:

Algorithm 5.1. (Relative enumeration)

Input: $q_{l,s}^{(i)}, C^{(i)}$ as above

Output: All $x \in M$ subject to $Q_i(x) \leq C^{(i)}$

Init: $l := m, T_l^{(i)} := C^{(i)}, U_l^{(i)} := 0$ ($1 \leq i \leq m$).

Step 1: $S_l := \{z \in \mathcal{O}_{\mathcal{E}} \mid |z^{(i)} - U_l^{(i)}|^2 \leq \frac{T_l^{(i)}}{q_{l,l}^{(i)}} \mid 1 \leq i \leq m\}$.

Step 2: If $S_l \neq \emptyset$ goto Step 4.

Step 3: Set $l := l + 1$, if $l > m$ then terminate else goto Step 2.

Step 4: Choose z_l in S_l arbitrary and delete z_l from S_l .

Step 5: If $l = 1$ print $x := \sum_{s=1}^n z_s \nu_s$ goto Step 2.

Step 6: $l := l - 1, T_l^{(i)} := T_{l+1}^{(i)} - q_{l+1,l+1}^{(i)} (z_{l+1}^{(i)} + U_{l+1}^{(i)})$, $U_l^{(i)} := \sum_{s=l+1}^n q_{l,s}^{(i)} z_s^{(i)}$, ($1 \leq i \leq m$) goto Step 1.

It remains to give an algorithm to compute the set S_l in Step 1. We will do this using a modified Fincke-Pohst algorithm. Instead of computing S_l , we compute a set $\tilde{S}_l := \{z \in \mathcal{O}_{\mathcal{E}} \mid \sum_{i=1}^m |z^{(i)} - U_l^{(i)}|^2 \leq \tilde{C}_l\}$ with $\tilde{C}_l := \sum_{i=1}^m \frac{T_l^{(i)}}{q_{l,l}^{(i)}}$. Let μ_1, \dots, μ_m be a \mathbb{Z} -basis of $\mathcal{O}_{\mathcal{E}}$ and define

$$W_l := \begin{pmatrix} \mu_1^{(1)} & \dots & \mu_m^{(1)} & U_l^{(1)} \\ \vdots & & \vdots & \vdots \\ \mu_1^{(m)} & \dots & \mu_m^{(m)} & U_l^{(m)} \end{pmatrix} \in \mathbb{C}^{m \times (m+1)}.$$

Now we have $\sum_{i=1}^m |x^{(i)} - U_l^{(i)}|^2 = (z_1, \dots, z_m, 1) \overline{W}_l^{\text{tr}} W_l (z_1, \dots, z_m, 1)^{\text{tr}}$ for every $x = \sum_{s=1}^m z_s \mu_s \in \mathcal{O}_{\mathcal{E}}$, $z_s \in \mathbb{Z}$. Clearly, $\overline{W}_l^{\text{tr}} W_l$ is positive semidefinite and real, so the \tilde{S}_l can be calculated with the classical Fincke-Pohst algorithm if we fix the last coordinate to be 1.

6. THE ALGORITHM

We are now able to present a complete algorithm for solving (4.2).

Algorithm 6.1. (Computing a complete set of nonassociate solutions of (4.2))

Input: $\theta \in o_{\mathcal{E}}, \gamma \in \mathbb{R}_{>0}^m, M$ and a complete set $\epsilon_1, \dots, \epsilon_r$ of independent units of the ring of multipliers of M .

Output: A complete set of nonassociate solutions of (4.2).

Init: Compute $\lambda_j = \lambda(\gamma_j, |\theta^{(j)}|)$ as in Lemma 3.2, $R_{(j-1)m+i}$ as in Lemma 4.1 and $L_i^{(j)}$ and $U_i^{(j)}$ as in Theorem 4.2. Let $S := \emptyset$.

Step 1: Compute $I := \{(r_i^{(j)})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \in \mathbb{Z}^{n \times m} \mid (2)-(4) \text{ of Theorem 4.2 hold}\}$.

Step 2: While $(I \neq \emptyset)$ do

Init enumeration: Choose $\mathbf{r} \in I$ arbitrary, and delete \mathbf{r} from I .

Enumerate: Determine all $\eta \in M$ satisfying (1) of Theorem 4.2 (e.g., using Algorithm 5.1).

Check: For each solution of the previous step, check (4.2). If we have a solution, check whether it is associated with one already in S . If we have a new solution, store it in S .

Step 3: If $S = \emptyset$ return “No solution” else return S .

In order to solve (4.1) instead of (4.2), one simply has to change the condition in “Check”. To estimate the algebraic complexity of this algorithm, we introduce the T_2 -norm: $T_2 : \mathcal{E} \rightarrow \mathbb{R} : \eta \mapsto \sum_{i=1}^m |\eta^{(i)}|^2$ and the so called “relative T_2 -norm” $T_{2,j}^{\mathcal{F}/\mathcal{E}} : \mathcal{F} \rightarrow \mathbb{R} : \eta \mapsto \sum_{i=1}^n |\eta^{((j-1)n+i)}|^2$ ($1 \leq j \leq m$).

Let ν_1, \dots, ν_n be an $o_{\mathcal{E}}$ -basis of M and ν_1^*, \dots, ν_n^* the corresponding dual basis subject to $\text{Tr}_{\mathcal{F}/\mathcal{E}}(\nu_i \nu_j^*) = \delta_{i,j}$. Define

$$d_j := \max_{1 \leq i \leq n} T_{2,j}^{\mathcal{F}/\mathcal{E}}(\nu_i^*) \quad (1 \leq j \leq m), \quad L_j := \max\{\lambda_j^{-r_i^{(j)}} \mid r \in I, 1 \leq i \leq n\},$$

$$C := \sum_{j=1}^m d_j L_j (n|\theta^{(j)}| + \gamma_j)^{2/n}.$$

Furthermore, let μ_1, \dots, μ_m be a \mathbb{Z} -basis of $o_{\mathcal{E}}$ and μ_1^*, \dots, μ_m^* its dual basis subject to $\text{Tr}_{\mathcal{E}/\mathbb{Q}}(\mu_i \mu_j^*) = \delta_{i,j}$. Let $d := \max_{1 \leq l \leq m} T_2(\mu_l^*)$.

We begin with the complexity of Algorithm 5.1.

Lemma 6.2. (1) *The algorithm for computing one set S_i in Step 1 of Algorithm 5.1 calculates $O\left((2\lfloor\sqrt{dC}\rfloor + 1)\left(\binom{\lfloor 4dC \rfloor + m - 1}{\lfloor 4dC \rfloor} + 1\right)\right)$ points. For each point it needs $O(m^2)$ operations, and additional $O(m^3)$ operations for precomputing.*

(2) *Algorithm 5.1 needs $O\left((mn^2 + m^3)\left((2\lfloor\sqrt{dC}\rfloor + 1)\left(\binom{\lfloor 4dC \rfloor + m - 1}{\lfloor 4dC \rfloor} + 1\right)\right)^n\right)$ operations.*

Proof. In the same way as in [3, Proof of 3.15] (cf. [4, Lemma 3.17] or [4, Lemma 4.13]) we normalize the task to $q_{l,l}^{(i)} \geq 1$. Now C is an upper bound for all S_i .

(1) Since we fix the last coordinate, we effectively enumerate an m -dimensional ellipsoid, so the statements follow at once from [3].

- (2) Clearly, we consider at most $O\left(\left((2\lfloor\sqrt{dC}\rfloor+1)\binom{\lfloor 4dC\rfloor+m-1}{\lfloor 4dC\rfloor}+1\right)^n\right)$ points, and for each point we need $O(mn^2+m^3)$ operations. \square

We note that we need $O(mn^3)$ operations for calculating the matrices B_i and the $q_{i,s}^{(i)}$.

Theorem 6.3. Define $D_j := 2\max_{1\leq i\leq n}\log R_{(j-1)n+i}$, $R_{(j-1)n+i}$ as in Lemma 4.1, $1\leq j\leq m$,

$$Q := mn^3 + (mn^2 + m^3) \left((2\lfloor\sqrt{dC}\rfloor + 1) \binom{\lfloor 4dC\rfloor + m - 1}{\lfloor 4dC\rfloor} + 1 \right)^n.$$

The set

$$I := \left\{ (r_i^{(j)})_{\substack{1\leq i\leq n \\ 1\leq j\leq m}} \in \mathbb{Z}^{n\times m} \mid (2)-(4) \text{ of Theorem 4.2 are valid} \right\}$$

contains at most

$$\prod_{j=1}^{m_1} (t_j + 1) \left(\frac{2}{\log \lambda_j} D_j + 3 \right)^{s_j + t_j - 1} \prod_{j=m_1+1}^{m_1+m_2} \left(\frac{2}{\log \lambda_j} D_j + 3 \right)^{n-1}$$

elements. For each $(r_i^{(j)})_{\substack{1\leq i\leq n \\ 1\leq j\leq m}} \in I$ (i.e., for each quadratic form considered) the algorithm needs $O(Q)$ arithmetic operations to enumerate all η with (1) of Theorem 4.2. Hence Algorithm 6.1 requires

$$O(\#\!I)Q$$

arithmetic operations.

Proof. See [4, Lemmas 4.12 and 4.13]. We note that the estimate for $\#\!I$ is a straightforward computation using only (2)–(4) of Theorem 4.2 and Lemma 4.1. \square

7. EXAMPLE

Let $\mathcal{E} := \mathbb{Q}(\alpha)$, α a zero of

$$f(x) := x^3 + 2x^2 - x + 2.$$

We consider the extension $\mathcal{F} := \mathcal{E}(\beta)$ of absolute degree 9, where β is a zero of

$$g(x) := x^3 + x^2 + (1 + 2\alpha + \alpha^2)x + (-2 + \alpha^2).$$

The signature of \mathcal{E} is $m_1 = m_2 = 1$. Since \mathcal{F} has only one real embedding, the unit rank of \mathcal{F} is 4. A system of fundamental units of $\mathcal{O}_{\mathcal{F}}$ is

$$\epsilon_1 := \frac{1}{2}(\alpha + \alpha^2),$$

$$\epsilon_2 := \frac{1}{2}(2 + 2\alpha + (2 - \alpha - \alpha^2)\beta),$$

$$\epsilon_3 := (-3 + \alpha^2 + (2 - 2\alpha - \alpha^2)\beta + (1 + \alpha)\beta),$$

$$\epsilon_4 := \frac{1}{2}(-20 + 5\alpha + 5\alpha^2 + (16 + 29\alpha + 9\alpha^2)\beta + (14 - 19\alpha - 9\alpha^2)\beta^2).$$

We consider the following problems:

- (1) Solve $|N_{\mathcal{F}/\mathbb{Q}}(x)| = k$ for $x \in o_{\mathcal{F}}$, $k \in \mathbb{Z}_{>0}$, using the absolute method. From Lemma 3.1 and Theorem 3.3 we obtain bounds (after an LLL-reduction of the unit lattice):

i		1	2	3	4	5	6	7	8	9
$-L_i = U_i$		18	14	18	14	7	14	18	14	7

This requires us to consider 328290 ellipsoids if all solutions of the norm equation are to be determined.

- (2) Solve $|N_{\mathcal{F}/\mathcal{E}}(x)| = |\theta|$ for $x \in o_{\mathcal{F}}$ and $\theta \in o_{\mathcal{E}}$ by
 - (a) the absolute method:

Lemma 4.1 and Theorem 3.3 yield bounds:

i		1	2	3	4	5	6	7	8	9
L_i		-14	-14	-11	-11	-19	-14	-11	-11	-19
U_i		13	15	10	11	20	15	10	11	20

A total of 494526 ellipsoids need to be enumerated.

- (b) the relative method:

Over $\mathcal{E}^{(1)}$ we have the relative signature $t_1 = s_1 = 1$. By Lemma 4.1 and Theorem 4.2 we obtain:

j		1			2			3		
i		1	2	3	1	2	3	1	2	3
$-L_i^{(j)} = U_i^{(j)}$		16	12	12	12	9	15	12	9	15

that is a total of only 14289 ellipsoids.

We note that we actually computed all these ellipsoids, so that the numbers L_i, U_i given above are exact.

8. TABLES

All computations were carried out on an HP9000/735s with 96MB memory using software developed under KANT V4 [5]. The operating system on the machine was HP-UX 9.01.

F. Grunewald in Düsseldorf asked us the following question: Let $\mathcal{E} = \mathbb{Q}(\alpha)$, $\alpha \in \{\sqrt{-1}, \sqrt{-2}, \sqrt{-3}\}$, $\beta = \sqrt{a + b\alpha}$ for $-3 \leq a, b \leq 3$ such that $\mathcal{F} = \mathcal{E}(\beta)$ is of absolute degree 4. How many nonassociate solutions do exist for (4.2) with “small” θ , where nonassociate means “modulo units of relative norm 1”? In Tables 1 and 2 we can only present a part of our results because of limited space.

Another problem of W. Plesken in Aachen and H. Brückner in Hamburg was to solve several norm equations in cyclotomic fields (see Table 3 for details). We present solutions of (4.1), “-” meaning that no solutions exist, and ζ_k denoting a primitive k th root of unity.

TABLE 1. Examples

\mathcal{E}	\mathcal{F}	θ	solution	rel. norm
$\mathbb{Q}(\sqrt{-2})$	$\mathcal{E}(\sqrt{-1})$	1	-1	1
			$\frac{1}{2}(\sqrt{-1}-1)\sqrt{-2}$	-1
		$\sqrt{-2}$	$\frac{1}{2}(2-\sqrt{-2}(1+\sqrt{-1}))$	$-\sqrt{-2}$
			$\frac{1}{2}(2\sqrt{-1}+\sqrt{-2}(1+\sqrt{-1}))$	$\sqrt{-2}$
		$-1 \pm \sqrt{-2}$	-	-
		3	$\pm 1 - \sqrt{-2}$	$-1 \mp 2\sqrt{-2}$
$\frac{1}{2}(2 \pm (1 - \sqrt{-1})\sqrt{-2} - 2\sqrt{-1})$	$1 \pm 2\sqrt{-2}$			
$\mathbb{Q}(\sqrt{-3})$	$\mathcal{E}(\sqrt{-1})$	1	-1	1
			$\frac{1}{2}(\pm 1 - \sqrt{-3})$	$\frac{1}{2}(-1 \mp \sqrt{-3})$
			$\frac{1}{2}(-2 + \sqrt{-1}(\pm 1 - \sqrt{-3}))$	$\frac{1}{2}(1 \mp \sqrt{-3})$
			$\frac{1}{2}(-1 + \sqrt{-3} - \sqrt{-1}(1 + \sqrt{-3}))$	-1
		$-1 - 2\sqrt{-3}$	$\frac{1}{2}(\mp 3 + \sqrt{-3} + \sqrt{-1}(\pm 1 - \sqrt{-3}))$	$1 \mp 2\sqrt{-3}$
			$\frac{1}{2}(2\sqrt{-3} + \sqrt{-1}(\pm 1 - \sqrt{-3}))$	$\frac{1}{2}(-7 \mp \sqrt{-3})$
			$\frac{1}{2}(\mp 3 + \sqrt{-3} - 2\sqrt{-1})$	$\frac{1}{2}(5 \mp 3\sqrt{-3})$
			$\frac{1}{2}(4 + \sqrt{-1}(\mp 1 + 3\sqrt{-3}))$	$\frac{1}{2}(-5 \mp 3\sqrt{-3})$
			$\frac{1}{2}(5 + 1\sqrt{-3} + \sqrt{-1}(-2 + 2\sqrt{-3}))$	$\frac{1}{2}(7 + \sqrt{-3})$
			$1 + \sqrt{-3} - \sqrt{-1}$	$-1 + 2\sqrt{-3}$
			$\frac{1}{2}(-1 + \sqrt{-3} - 4\sqrt{-1})$	$\frac{1}{2}(7 - \sqrt{-3})$
			$1 - \sqrt{-1}(-1 + \sqrt{-3})$	$-1 - 2\sqrt{-3}$

TABLE 2. Examples

\mathcal{E}	\mathcal{F}	β	solution	rel. norm	
$\mathbb{Q}(\sqrt{-1})$	$\mathcal{E}(\sqrt{2})$	1	-1	1	
			$\frac{1}{2}\sqrt{2}(\pm 1 - \sqrt{-1})$	$\pm\sqrt{-1}$	
			$\sqrt{-1}$	-1	
		$1 + \sqrt{-1}$	$\frac{1}{2}(2\sqrt{-1} + \sqrt{-2}(\mp 1 + \sqrt{-1}))$	$-1 \pm \sqrt{-1}$	
			$\frac{1}{2}(\pm 2 + \sqrt{-2}(\pm 1 - \sqrt{-1}))$	$1 \pm \sqrt{-1}$	
		-2 ± 1	-	-	
		-5	$\frac{1}{2}\sqrt{2}(-3 \pm \sqrt{-1})$	$-4 \pm 3\sqrt{-1}$	
			$\frac{1}{2}\sqrt{2}(\pm 1 - 3\sqrt{-1})$	$4 \pm 3\sqrt{-1}$	
			$\pm 2 - \sqrt{-1}$	$3 \mp 4\sqrt{-1}$	
			$\pm 1 - 2\sqrt{-1}$	$-3 \mp 4\sqrt{-1}$	
		$\mathcal{E}(\sqrt{\sqrt{-1}})$	-1	-1	1
				$-\sqrt{\sqrt{-1}}$	$\sqrt{-1}$
	$-\sqrt{-1}$			-1	
	$-\sqrt{-1}\sqrt{\sqrt{-1}}$			$-\sqrt{-1}$	
	$1 + \sqrt{-1}$		$-\sqrt{-1} - \sqrt{-1}\sqrt{\sqrt{-1}}$	$-1 + \sqrt{-1}$	
			$\sqrt{-1} + \sqrt{\sqrt{-1}}$	$-1 - \sqrt{-1}$	
			$1 - \sqrt{-1}\sqrt{\sqrt{-1}}$	$1 + \sqrt{-1}$	
			$-1 - \sqrt{-1}$	$1 - \sqrt{-1}$	
	$\mathcal{E}(\sqrt{1 + \sqrt{-1}})$	1	-1	1	
			$-\sqrt{-1}$	-1	
			$1 + \sqrt{1 + \sqrt{-1}}$	$-\sqrt{-1}$	
			$-\sqrt{-1} - \sqrt{-1}\sqrt{1 + \sqrt{-1}}$	$\sqrt{-1}$	
		$1 + \sqrt{-1}$	$-\sqrt{1 + \sqrt{-1}}$	$-1 - \sqrt{-1}$	
			$-\sqrt{-1}\sqrt{1 + \sqrt{-1}}$	$1 + \sqrt{-1}$	
			$-1 - \sqrt{-1} - \sqrt{1 + \sqrt{-1}}$	$-1 + \sqrt{-1}$	
			$-1 + \sqrt{-1} + \sqrt{-1}\sqrt{1 + \sqrt{-1}}$	$1 - \sqrt{-1}$	

TABLE 3. Examples

\mathcal{E}	\mathcal{F}	β	solution
$\mathbb{Q}(\zeta_5) \cap \mathbb{R}$	$\mathbb{Q}(\zeta_5)$	$2 - \zeta_4 - \zeta_5^{-1}$	$1 - \zeta_5$
		-1	$-$
$\mathbb{Q}(\zeta_7) \cap \mathbb{R}$	$\mathbb{Q}(\zeta_7)$	$2 - \zeta_7 - \zeta_7^{-1}$	$1 - \zeta_7$
		-1	$-$
$\mathbb{Q}(\zeta_8) \cap \mathbb{R}$	$\mathbb{Q}(\zeta_8)$	$2 - \zeta_8 - \zeta_8^{-1}$	$1 - \zeta_8$
		-1	$-$
$\mathbb{Q}(\zeta_9) \cap \mathbb{R}$	$\mathbb{Q}(\zeta_9)$	$2 - \zeta_9 - \zeta_9^{-1}$	$1 - \zeta_9$
		-1	$-$
$\mathbb{Q}(\zeta_{10}) \cap \mathbb{R}$	$\mathbb{Q}(\zeta_{10})$	$2 - \zeta_{10} - \zeta_{10}^{-1}$	$1 - \zeta_{10}$
		-1	$-$
$\mathbb{Q}(\zeta_{11}) \cap \mathbb{R}$	$\mathbb{Q}(\zeta_{11})$	$2 - \zeta_{11} - \zeta_{11}^{-1}$	$1 - \zeta_{11}$
		-1	$-$
$\mathbb{Q}(\zeta_{12}) \cap \mathbb{R}$	$\mathbb{Q}(\zeta_{12})$	$2 - \zeta_{12} - \zeta_{12}^{-1}$	$1 - \zeta_{12}$
		-1	$-$
$\mathbb{Q}(\zeta_{16}) \cap \mathbb{R}$	$\mathbb{Q}(\zeta_{16})$	-1	$-$
$\mathbb{Q}(\zeta_{32}) \cap \mathbb{R}$	$\mathbb{Q}(\zeta_{32})$	-1	$-$
$\mathbb{Q}(\zeta_{64}) \cap \mathbb{R}$	$\mathbb{Q}(\zeta_{64})$	-1	$-$

REFERENCES

1. U. Fincke, *Ein Ellipsoidverfahren zur Lösung von Normgleichungen in algebraischen Zahlkörpern*, Thesis, Düsseldorf 1984.
2. U. Fincke, M. Pohst, *A Procedure for Determining Algebraic Integers of Given Norm*, Proceedings EUROCAL 83, Springer Lecture Notes in Computer Science No. 162, Springer, 1983. MR **86k**:11078
3. U. Fincke, M. Pohst, *Improved methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis*, Math. Comp. 44, 463–471 (1985). MR **86e**:11050
4. A. Jurk, *Über die Berechnung von Lösungen relativer Normgleichungen in algebraischen Zahlkörpern*, Thesis, Düsseldorf 1993.
5. The Kant-Group, *KANT V4*, to appear in J. Symb. Comput.
6. K. Mahler, *Inequalities for Ideal Bases in Algebraic Number Fields*, J. Austral. Math. Soc. 4, 425–447 (1964). MR **31**:1243
7. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer, 1990. MR **91h**:11107
8. M. Pohst, H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Encyclopaedia of Mathematics and its Applications, Cambridge University Press, 1989. MR **92b**:11074

FACHBEREICH 3 MATHEMATIK, SEKRETARIAT MA 8–1, TECHNISCHE UNIVERSITÄT BERLIN,
STRASSE DES 17. JUNI 136, D-10623 BERLIN, GERMANY
E-mail address: fieker@math.tu-berlin.de

DESDORFER WEG 15, 50181 BEDBURG, GERMANY

FACHBEREICH 3 MATHEMATIK, SEKRETARIAT MA 8–1, TECHNISCHE UNIVERSITÄT BERLIN,
STRASSE DES 17. JUNI 136, D-10623 BERLIN, GERMANY
E-mail address: pohst@math.tu-berlin.de