Publ. Math. Debrecen
56 / 3-4 (2000), 375–390

An efficient algorithm for the explicit resolution of norm form equations

By ISTVÁN GAÁL (Debrecen)

Dedicated to Professor Kálmán Győry on his 60th birthday

Abstract. We give an efficient method for the explicit resolution of norm form equations under general assumptions. The main tool is the application of Wildanger's enumeration algorithm [14], more exactly an appropriate version of it described by GAÁL and POHST [8].

1. Introduction

Although there is an extensive literature of the explicite resolution of Thue equations, see e.g. PETHŐ and SCHULENBERG [10], TZANAKIS and de WEGER [13], BILU and HANROT [2], SMART [12], GAÁL and POHST [8], and index form equations, cf. GAÁL [6], [7] for a survey, the problem of solving norm form equations was not yet investigated. Our purpose is now to fill this gap and to give an efficient method for solving norm form equations under general conditions.

Let $\alpha_1 = 1, \alpha_2, \dots, \alpha_m$ be algebraic integers, linearly independent over $\mathbb{Q}$, let $K = \mathbb{Q}(\alpha_2, \dots, \alpha_m)$, $L = \mathbb{Q}(\alpha_1, \dots, \alpha_{m-1})$, and assume that

$$[K : L] \geq 3. \tag{1}$$

Mathematics Subject Classification: 11Y50, 11D57.
Key words and phrases: norm form equations, explicit resolution.
Research supported in part by Grants 16975 and 25157 from the Hungarian National Foundation for Scientific Research.

Let $0 \neq b \in \mathbb{Z}$ and consider the *norm form equation*

$$(2)\ \ N_{K/\mathbb{Q}}(x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m) = d \quad \text{in } x_1, x_2, \ldots, x_m \in \mathbb{Z},\ x_m \neq 0.$$

Using Baker's method GYŐRY gave effective upper bounds for the solutions of norm form equations of the above type, cf. e.g. [9] (see [3] for improved bounds), reducing the equation to unit equations in two variables. Some of his ideas are used also in this paper. In order to apply Baker's method it was necessary to make assumptions on the coefficients: (1) was the most general assumption of these.

Note that SMART [11] gave a method for solving triangularly connected decomposable form equations, which involve also some special norm form equations, but his purpose was not to consider norm form equations utilizing their special properties, hence his general method is not feasible for norm form equations of the above type.

The purpose of the present paper is to work out an efficient algorithm for the explicite resolution of equation (2). In the course of our method we need to use Baker's method, hence we also have to assume (1). In fact we reduce the problem to solving a special type of relative Thue equation over L. One of our gools is to show that by solving equation (2) it is sufficient to deal with linear forms in $r(K) - r(L)$ variables, where $r(K)$ resp. $r(L)$ denote the unit rank of K resp. L. The second gool is to show, that the enumeration method of GAÁL and POHST [8] (which is in fact an appropriate version of WILDANGER's enumeration [14]) can be applied in its original form. This way we become an efficient method for the enumeration of small exponents in the corresponding unit equation for reasonable values (up to about 11) of $r(k) - r(L)$.

2. Preliminaries

Let $l = [L : \mathbb{Q}]$, $k = [K : L]$ and denote by $\gamma^{(ij)}$ $(1 \leq i \leq l,\ 1 \leq j \leq k)$ the conjugates of any $\gamma \in K$ so that $\gamma^{(i1)}, \ldots, \gamma^{(ik)}$ are just corresponding relative conjugates of γ over the conjugate field $L^{(i)}$ of L. For elements μ of L we write $\mu^{(i)}$ for $\mu^{(i1)} = \ldots = \mu^{(ik)}$.

Assume that $\eta_1, \ldots, \eta_s$ is a set of fundamental units in L. Let us extend this system to a system of independent units $\eta_1, \ldots, \eta_s, \varepsilon_1, \ldots, \varepsilon_r$ of full rank in K. Denote by q the index of the unit group generated by these units in the whole unit group of K.

Calculate a full set of non-associated integers ν of K of norm $\pm d$. The algorithm must be performed for each element ν of this set.

Assume that $\underline{x} = (x_1, \dots, x_m) \in \mathbb{Z}^m$ is a solution of (2). Let $l(\underline{x}) = x_1 + \alpha_2 x_2 + \dots + \alpha_m x_m$. For $1 \le i \le l$, $1 \le j \le k$ we have

$$\begin{aligned} l^{(ij)}(\underline{x}) &= x_1 + \alpha_2^{(i)} x_2 + \dots + \alpha_{m-1}^{(i)} x_{m-1} + \alpha_m^{(ij)} x_m \\ &= \zeta_{ij} \nu^{(ij)} \left(\eta_1^{(i)}\right)^{\frac{b_1}{q}} \dots \left(\eta_s^{(i)}\right)^{\frac{b_s}{q}} \left(\varepsilon_1^{(ij)}\right)^{\frac{a_1}{q}} \dots \left(\varepsilon_r^{(ij)}\right)^{\frac{a_r}{q}} \end{aligned} \tag{3}$$

with some integers $b_1, \dots, b_s, a_1, \dots, a_r \in \mathbb{Z}$, where ζ_{ij} is a root of unity and we use throughout a fixed determination of the q-th root of the numbers involved. For any i $(1 \le i \le l)$ and distinct j_1, j_2, j_3 $(1 \le j_1, j_2, j_3 \le k)$ we have

$$\begin{aligned} \left(\alpha_m^{(ij_1)} - \alpha_m^{(ij_2)}\right) l^{(ij_3)}(\underline{x}) + \left(\alpha_m^{(ij_2)} - \alpha_m^{(ij_3)}\right) l^{(ij_1)}(\underline{x}) \\ + \left(\alpha_m^{(ij_3)} - \alpha_m^{(ij_1)}\right) l^{(ij_2)}(\underline{x}) = 0 \end{aligned}$$

whence

$$\frac{\alpha_m^{(ij_2)} - \alpha_m^{(ij_3)}}{\alpha_m^{(ij_1)} - \alpha_m^{(ij_3)}} \cdot \frac{l^{(ij_1)}(\underline{x})}{l^{(ij_2)}(\underline{x})} + \frac{\alpha_m^{(ij_2)} - \alpha_m^{(ij_1)}}{\alpha_m^{(ij_3)} - \alpha_m^{(ij_1)}} \cdot \frac{l^{(ij_3)}(\underline{x})}{l^{(ij_2)}(\underline{x})} = 1$$

that is

$$\begin{aligned} &\frac{\left(\alpha_m^{(ij_2)} - \alpha_m^{(ij_3)}\right) \zeta_{ij_1} \nu^{(ij_1)}}{\left(\alpha_m^{(ij_1)} - \alpha_m^{(ij_3)}\right) \zeta_{ij_2} \nu^{(ij_2)}} \left(\frac{\varepsilon_1^{(ij_1)}}{\varepsilon_1^{(ij_2)}}\right)^{\frac{a_1}{q}} \dots \left(\frac{\varepsilon_r^{(ij_1)}}{\varepsilon_r^{(ij_2)}}\right)^{\frac{a_r}{q}} \\ &+ \frac{\left(\alpha_m^{(ij_2)} - \alpha_m^{(ij_1)}\right) \zeta_{ij_3} \nu^{(ij_3)}}{\left(\alpha_m^{(ij_3)} - \alpha_m^{(ij_1)}\right) \zeta_{ij_2} \nu^{(ij_2)}} \left(\frac{\varepsilon_1^{(ij_3)}}{\varepsilon_1^{(ij_2)}}\right)^{\frac{a_1}{q}} \dots \left(\frac{\varepsilon_r^{(ij_3)}}{\varepsilon_r^{(ij_2)}}\right)^{\frac{a_r}{q}} = 1. \end{aligned} \tag{4}$$

This is the unit equation we are going to solve using the method described in [8]. The only difference between this equation and the equation considered in [8] is that here in the exponents we have a denominator q.

Introduce

$$\gamma^{(ij_1j_2j_3)} = \frac{\left(\alpha^{(ij_2)} - \alpha^{(ij_3)}\right) \zeta_{ij_1} \nu^{(ij_1)}}{\left(\alpha^{(ij_1)} - \alpha^{(ij_3)}\right) \zeta_{ij_2} \nu^{(ij_2)}}, \quad \rho_k^{(ij_1j_2)} = \left(\frac{\varepsilon_k^{(ij_1)}}{\varepsilon_k^{(ij_2)}}\right)^{\frac{1}{q}} \quad (1 \le k \le r)$$

and

$$\tau^{(ij_1j_2)} = \left(\rho_1^{(ij_1j_2)}\right)^{a_1} \dots \left(\rho_r^{(ij_1j_2)}\right)^{a_r},$$

then we have

$$\beta^{(ij_1j_2j_3)} = \frac{\alpha_m^{(ij_2)} - \alpha_m^{(ij_3)}}{\alpha_m^{(ij_1)} - \alpha_m^{(ij_3)}} \cdot \frac{l^{(ij_1)}(\underline{x})}{l^{(ij_2)}(\underline{x})} = \gamma^{(ij_1j_2j_3)}\tau^{(ij_1j_2)}.$$

for any i $(1 \leq i \leq l)$ and any distinct $j_1,\ j_2,\ j_3$ $(1 \leq j_1, j_2, j_3 \leq k)$. Equation (4) can be written in the form

$$\beta^{(ij_1j_2j_3)} + \beta^{(ij_3j_2j_1)} = 1. \tag{5}$$

We use the algorithm of [8] to solve equation (5) in $a_1, \dots, a_r$. For the sake of completeness we give here a brief sketch of the procedure.

3. Solving the unit equation

We only summarize the main steps.

1. Elementaries. By solving the system of linear equations

$$a_1 \log\left|\rho_1^{(ij_1j_2)}\right| + \ldots + a_r \log\left|\rho_r^{(ij_1j_2)}\right| = \log\left|\tau^{(ij_1j_2)}\right| \tag{6}$$

in $a_1, \dots, a_r$ $(1 \leq i \leq l,\ \ 1 \leq j_1, j_2 \leq k,\ \ j_1 \neq j_2)$, we obtain

$$A = \max(|a_1|, \dots, |a_r|) \leq c_1 \cdot \left|\log\left|\tau^{(ij_1j_2)}\right|\right| \tag{7}$$

for a certain set i, j_1, j_2 of indices. Exchanging j_1 and j_2 if necessary, (7) implies that there are indices i, j_1, j_2 with

$$\left|\tau^{(ij_1j_2)}\right| < \exp\left(-\frac{A}{c_1}\right). \tag{8}$$

The following steps must be performed for all possible values of i, j_1, j_2.

2. Baker's method. Let $1 \leq j_3 \leq k$ be any index distinct from j_1, j_2. Applying (8) from (5) we get

$$\left|\log\left(\beta^{(ij_3j_2j_1)}\right)\right| \leq 2\cdot\left|\beta^{(ij_3j_2j_1)} - 1\right| = 2\cdot\left|\beta^{(ij_1j_2j_3)}\right| \leq c_2 \exp\left(-\frac{A}{c_1}\right). \tag{9}$$

On the other hand,

$$\left|\log\left(\beta^{(ij_3j_2j_1)}\right)\right| = \left|\log\left(\gamma^{(ij_3j_2j_1)}\right) + a_1\cdot\log\left(\rho_1^{(ij_3j_2)}\right) + \ldots + a_r\cdot\log\left(\rho_r^{(ij_3j_2)}\right) + a_0\cdot\log(-1)\right| \tag{10}$$

where log denotes the principal value of the logarithm, and $a_0 \in \mathbb{Z}$ with $|a_0| \le |a_1| + \ldots + |a_r| + 1$. Set $A' = \max(|a_1|, \ldots, |a_r|, |a_0|)$, then $A \le A' \le rA + 1$. In case the terms in the above linear form are independent (otherwise we can reduce the number of variables) using the estimates of Baker and Wüstholz [1] and (9) we conclude

$$\exp(-C\cdot\log A') \le \left|\log\left(\beta^{(ij_3j_2j_1)}\right)\right| \le c_2\exp\left(-\frac{A'+1}{rc_1}\right) \tag{11}$$

which implies an upper bound A'_B for A' of magnitude 10^{20} up to 10^{500} for $r = 2$ up to 8.

3. Reduction. Using (10) and (11) we have an estimate of type

$$|\xi + a_1\xi_1 + \ldots + a_r\xi_r + a_0\xi_0| < c_2\exp(-c_3A' - c_4) \tag{12}$$

where

$$\begin{aligned}\xi &= \log\left(\gamma^{(ij_3j_2j_1)}\right), \quad \xi_1 = \log\left(\rho_1^{(ij_3j_2)}\right), \ \ldots, \\ \xi_r &= \log\left(\rho_r^{(ij_3j_2)}\right), \quad \xi_0 = \log(-1).\end{aligned}$$

Let H be a large constant to be specified later. Consider the lattice $\mathcal{L}$ spanned be the columns of the matrix

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 1 \\ H\Re(\xi) & H\Re(\xi_1) & \ldots & H\Re(\xi_r) & H\Re(\xi_0) \\ H\Im(\xi) & H\Im(\xi_1) & \ldots & H\Im(\xi_r) & H\Im(\xi_0) \end{pmatrix}.$$

Assume, that the columns in the above matrix are linearly independent. Denote by b_1 the first vector of the LLL-reduced basis of this lattice. The reduction procedure is based on Lemma 1 of [8]:

Lemma 1. *If $A' \le A'_0$ and $|b_1| \ge \sqrt{(r+3)2^{r+1}} \cdot A'_0$ then*

$$A' \le \frac{\log H + \log c_2 - c_4 - \log A'_0}{c_3}.$$

If the field K is totally real, we can omit the variable corresponding to a_0 and the imaginary parts in the last component of the generating vectors of the lattice $\mathcal{L}$. We first take A'_0 to be the Baker's bound A'_B, apply the lemma to reduce it, and in the next step we use the new bound in the role of A'_0. An appropriate value of H corresponding to A'_0 is of magnitude $(A'_0)^{r+2}$. We need about 4–5 reduction steps. The final reduced bound A'_R is usually between 100 and 1000.

4. Enumeration. Let $I = (i, j_1, j_2, j_3)$ be a tuple with $1 \le i \le l$, $1 \le j_1, j_2, j_3 \le k$ so that j_1, j_2, j_3 are distinct. Introduce

$$\beta^{(I)} = \beta^{(ij_1j_2j_3)}, \quad \gamma^{(I)} = \gamma^{(ij_1j_2j_3)}, \quad \rho_h^{(I)} = \rho_h^{(ij_1j_2)} \quad (1 \le h \le r).$$

Let $I^* = \{I_1, \dots, I_t\}$ be a set of tuples I with the following properties:

1. if $(ij_1j_2j_3) \in I^*$ then either $(ij_2j_3j_1) \in I^*$ or $(ij_3j_2j_1) \in I^*$
2. if $(ij_1j_2j_3) \in I^*$ then either $(ij_1j_3j_2) \in I^*$ or $(ij_3j_1j_2) \in I^*$
3. the vectors $\underline{e}_h = \left(\log\left|\rho_h^{(I_1)}\right|, \dots, \log\left|\rho_h^{(I_t)}\right|\right)$ $(1 \le h \le r)$ are linearly independent.

Set $\underline{g} = \left(\log\left|\gamma^{(I_1)}\right|, \dots, \log\left|\gamma^{(I_t)}\right|\right)$ and $\underline{b} = \left(\log\left|\beta^{(I_1)}\right|, \dots, \log\left|\beta^{(I_t)}\right|\right)$. By our notation we have

$$\underline{b} = \underline{g} + a_1\underline{e}_1 + \dots + a_r\underline{e}_r. \tag{13}$$

Using the reduced bound A'_R we can calculate a constant S with

$$\frac{1}{S} \le \left|\beta^{(I)}\right| \le S \quad \text{for all } I \in I^*. \tag{14}$$

In order to replace S by a smaller constant s we use Lemma 2 of [8]:

Lemma 2. *Let $2 < s < S$ be given constants and assume that* (14) *holds. Then either*

$$\frac{1}{s} \le \left|\beta^{(I)}\right| \le s \quad \textit{for all} \quad I \in I^* \tag{15}$$

or there is an $I_{j_0} \in I^*$ *with*

$$\left|\beta^{(I_{j_0})} - 1\right| \le \frac{1}{s-1}. \tag{16}$$

Hence, the constant S can be replaced by the smaller constant s if for each j_0 $(1 \le j_0 \le t)$ we enumerate directly the set H_{j_0} of those exponents $a_1, \dots, a_r$ for which (14) and (16) hold. For $1 \le j \le t$ set $\lambda_j = 1/\log S$ for $j \ne j_0$ and set $\lambda_{j_0} = 1/\log \frac{s-1}{s-2}$. Further, let $\lambda_{t+1} = 1/\arccos \frac{s(s-2)}{(s-1)^2}$. Set

$$\varphi_{j_0}(\underline{b}) = \left(\lambda_1 \log\left|\beta^{(I_1)}\right|, \dots, \lambda_t \log\left|\beta^{(I_t)}\right|, \lambda_{t+1} \arg\left(\beta^{(I_{j_0})}\right)\right),$$

$$\varphi_{j_0}(\underline{g}) = \left(\lambda_1 \log\left|\gamma^{(I_1)}\right|, \dots, \lambda_t \log\left|\gamma^{(I_t)}\right|, \lambda_{t+1} \arg\left(\gamma^{(I_{j_0})}\right)\right),$$

$$\varphi_{j_0}(\underline{e}_h) = \left(\lambda_1 \log\left|\rho_h^{(I_1)}\right|, \dots, \lambda_t \log\left|\rho_h^{(I_t)}\right|, \lambda_{t+1} \arg\left(\rho_h^{(I_{j_0})}\right)\right) \quad (1 \le h \le r),$$

where for any $z \in \mathbb{C}$ the inequality $-\pi \le \arg z \le \pi$ is satisfied and let $\underline{e}_0 = (0, \dots, 0, \pi) \in \mathbb{R}^{t+1}$. By (13) we have

$$\varphi_{j_0}(\underline{b}) = \varphi_{j_0}(\underline{g}) + a_1\varphi_{j_0}(\underline{e}_1) + \dots + a_r\varphi_{j_0}(\underline{e}_r) + a_0\underline{e}_0. \tag{17}$$

Moreover, for the norm of this vector we have

$$\begin{aligned} &\|\varphi_{j_0}(\underline{g}) + a_1\varphi_{j_0}(\underline{e}_1) + \dots + a_r\varphi_{j_0}(\underline{e}_r) + a_0\underline{e}_0\|_2^2 = \|\varphi_{j_0}(\underline{b})\|_2^2 \\ &\quad = \sum_{j=1}^{t} \lambda_j^2 \log^2\left|\beta^{(I_j)}\right| + \lambda_{t+1}^2 \arg^2\left(\beta^{(I_{j_0})}\right) \le t+1. \end{aligned} \tag{18}$$

This inequality defines an ellipsoid. The lattice points contained in this ellipsoid can be enumerated by using the algorithm of Fincke and Pohst [5]. The enumeration is usually very fast, but it is essential, that the "improved" version of the algorithm should be used, involving LLL reduction. If K is totally real, the $(t+1)$-st component of φ_{j_0}, the vector $\underline{e}_0$ and the variable a_0 can be omitted, and in (18) we only get t on the right side. We usually apply the lemma about 5–10 times, until the final s is as small as possible, so that the exponents with (15) can be enumerated easily.

Observe, that this set is also contained in an ellipsoid, namely, by (13) we have in $\mathbb{R}^t$

$$\|\underline{g} + a_1\underline{e}_1 + \ldots + a_r\underline{e}_r\|_2^2 = \|\,\underline{b}\,\|_2^2 \le t\cdot s^2. \tag{19}$$

4. Calculating the solutions of the norm form equation

The procedure of the preceeding section gives us all possible tuples $(a_1,\ldots,a_r)$ of exponents in (3). For any i,j $(1\le i\le l,\ 1\le j\le k)$ set

$$\delta^{(i)} = \left(\eta_1^{(i)}\right)^{\frac{b_1}{q}} \cdots \left(\eta_s^{(i)}\right)^{\frac{b_s}{q}}$$

and

$$\gamma^{(ij)} = \zeta_{ij}\,\nu^{(ij)}\left(\varepsilon_1^{(ij)}\right)^{\frac{a_1}{q}} \cdots \left(\varepsilon_r^{(ij)}\right)^{\frac{a_r}{q}}.$$

The $\delta^{(i)}$ are not yet known, but the $\gamma^{(ij)}$ are determined by the exponents $(a_1,\ldots,a_r)$. Then we have

$$l^{(ij)}(\underline{x}) = x_1 + \alpha_2^{(i)}x_2 + \ldots + \alpha_{m-1}^{(i)}x_{m-1} + \alpha_m^{(ij)}x_m = \delta^{(i)}\gamma^{(ij)}. \tag{20}$$

For any $1 < i \le l$ we have

$$\delta^{(i)}\left(\gamma^{(i1)} - \gamma^{(i2)}\right) = l^{(i1)}(\underline{x}) - l^{(i2)}(\underline{x}) = \left(\alpha_m^{(i1)} - \alpha_m^{(i2)}\right)x_m,$$

hence

$$0 \ne x_m = \delta^{(i)}\frac{\gamma^{(i1)} - \gamma^{(i2)}}{\alpha_m^{(i1)} - \alpha_m^{(i2)}}$$

that is

$$\delta^{(i)} = \tau_i\delta^{(1)} \tag{21}$$

with

$$\tau_1 = 1, \quad \tau_i = \frac{\alpha_m^{(i1)} - \alpha_m^{(i2)}}{\gamma^{(i1)} - \gamma^{(i2)}}\,\frac{\gamma^{(11)} - \gamma^{(12)}}{\alpha_m^{(11)} - \alpha_m^{(12)}} \quad \text{for } i = 2,\ldots,l.$$

Substituting our expressions into the original equation (2) it can be written in the form

$$\prod_{i=1}^{l}\prod_{j=1}^{k} l^{(ij)}(\underline{x}) = d,$$

whence we obtain

$$\prod_{i=1}^{l}\prod_{j=1}^{k}\left(\tau_i \delta^{(1)} \gamma^{(ij)}\right) = d,$$

that is

$$\left(\delta^{(1)}\right)^{kl} = d\left(\prod_{i=1}^{l}\prod_{j=1}^{k}\gamma^{(ij)}\right)^{-1}\left(\prod_{i=1}^{l}\tau_i\right)^{-k}, \tag{22}$$

from which we can calculate the value of $\delta^{(1)}$. This gives at once the value of $\delta^{(i)}$ by (21). Finally, solving the system of linear equations (20) $(1 \le i \le l,\ 1 \le j \le k)$ in $x_1, \dots, x_m$ we get the solutions of equation (2).

5. Example 1

We illustrate our algorithm by a two detailed examples. The basic number field data were calculated by using Kash [4]. The program was developed in Maple and was executed on a Pentium II PC.

Consider first the field K generated by a root ξ of the polynomial

$$f(x) = x^9 - x^8 - 31x^7 + 8x^6 + 200x^5 - 87x^4 - 97x^3 + 27x^2 + 12x - 1.$$

This field is totally real and has an integral basis

$$\{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7, \omega_9\}$$

with

$$\omega_9 = \big(14800 + 24483\xi + 15778\xi^2 + 15468\xi^3 + 19731\xi^4 + 4153\xi^5 + 1420\xi^6 + 4197\xi^7 + \xi^8\big)/25349.$$

The discriminant of the field is $D_K = 107226034120512 = 2^6 \cdot 3^3 \cdot 37^3 \cdot 107^3$.

The field K has a totally real cubic subfield L generated by α defined by the polynomial $g(x) = x^3 - x^2 - 3x + 1$ with discriminant $D_L = 148 =$

$2^2 \cdot 37$. (Note that K has also another cubic subfield generated by the root of $x^3 - x^2 - 4x + 1$ with discriminant $321 = 3 \cdot 107$ but this is not interesting in our arguments.) The field L has integral basis $\{1, \alpha, \alpha^2\}$ and fundamental units

$$\eta_1 = \alpha \quad \eta_2 = 2\alpha - 1.$$

These elements have the following coefficients in the integral basis of K:

$$\eta_1 = [-430, -703, -454, -472, -568, -117, -42, -122, 736]$$

$$\eta_2 = [-6383, -10561, -6838, -6694, -8428, -1791, -626, -1811, 10936].$$

These units together with

$$\varepsilon_1 = [328, 539, 346, 360, 433, 89, 32, 93, -561]$$

$$\varepsilon_2 = [758, 1242, 800, 832, 1001, 206, 74, 215, -1297]$$

$$\varepsilon_3 = [3590, 5940, 3838, 3746, 4739, 1010, 352, 1018, -6148]$$

$$\varepsilon_4 = [6055, 10022, 6492, 6334, 7995, 1702, 594, 1718, -10375]$$

$$\varepsilon_5 = [103, 164, 108, 112, 135, 28, 10, 29, -175]$$

$$\varepsilon_6 = [6225, 10295, 6682, 6551, 8218, 1745, 611, 1767, -10670].$$

form a system of fundamental units in K. (Hence $s = 2$, $r = 6$, $q = 1$.)

Consider the norm form equation

$$\begin{aligned} &N_{K/\mathbb{Q}}(x_1 + \alpha x_2 + \alpha^2 x_3 + \xi x_4) = \pm 1 \\ &\text{in } x_1, x_2, x_3, x_4 \in \mathbb{Z} \quad \text{with } x_4 \neq 0. \end{aligned} \tag{23}$$

We had $c_1 = 0.763$ and $c_2 = 4.291$ for all possible i, j_1, j_2. Since our example is a totally real one, we did not have to use a_0. Baker's method gave

$$A = \max(|a_1|, \ldots, |a_6|) \leq 10^{36} = A_B.$$

In the reduction procedure we had dimension 7, $c_3 = 1/c_1$, $c_4 = 0$. The following table summarizes the steps of the reduction procedure. Note that in each step we had to perform 9 reductions.

	$A <$	$\lvert b_1\rvert >$	$H =$	precision	new bound for A	CPU time
Step I	10^{36}	10^{39}	10^{280}	700 digits	429	20 min
Step II	429	9709	10^{30}	100 digits	49	8 sec
Step III	49	1109	10^{22}	60 digits	36	5 sec
Step IV	36	815	10^{21}	60 digits	35	5 sec

Hence our algorithm gave the reduced bound $A_R = 35$.

In the enumeration process we used

$$I^* = \{(i123), (i231), (i312) \mid i = 1, 2, 3\}$$

that is we had $t = 9$ ellipsoids to consider. The initial bound was $S = 0.4116 \cdot 10^{153}$ that we got using the reduced bound for A. Note that in this example the vector $\underline{g}$ is linearly dependent on $\underline{e}_1, \ldots, \underline{e}_6$. The following table is a summary of the enumeration process.

	S	s	precision	CPU time	tuples found
Step I	10^{153}	10^{20}	100 digits	10 sec	0
Step II	10^{20}	10^{10}	50 digits	5 sec	0
Step III	10^{10}	10^{8}	50 digits	4 sec	0
Step IV	10^{8}	10^{6}	50 digits	4 sec	2
Step V	10^{6}	10^{5}	50 digits	3 sec	8
Step VI	10^{5}	10^{4}	50 digits	3 sec	16
Step VII	10^{4}	10^{3}	50 digits	3 sec	34
Step VIII	10^{3}	10^{2}	50 digits	3 sec	96
Step IX	10^{2}	10	50 digits	3 sec	133
Step X	10	5	50 digits	5 sec	15
Step XI	5	3	50 digits	5 sec	15
Step XII	3		50 digits	3 sec	34

The last line refers to the enumeration of the ellipsoid (19) with $s = 3$.

We tested all tuples we found in the enumeration process if they are solutions of (4). We found 14 solutions of (4), the components were all ≤ 2 in absolute value. For these tuples we calculated the corresponding solutions of the equation (23). We obtained the following solutions:

x_1	x_2	x_3	x_4
0	0	0	-1
0	0	1	-1
1	-1	-1	1
0	-1	1	1
1	-1	0	-1
-1	0	1	1
0	2	-1	1
-1	-2	0	1

If (x_1, x_2, x_3, x_4) is a solution then so also is $(-x_1, -x_2, -x_3, -x_4)$ but we list only one of them.

6. Example 2

Our second example refers to a more complicated situation. Consider the field K generated by a root ξ of the polynomial

$$\begin{aligned} f(x) = x^{12} - 80x^{10} - 85x^9 + 568x^8 + 184x^7 - 1041x^6 + 40x^5 \\ + 432x^4 - 19x^3 - 52x^2 - 2x + 1. \end{aligned}$$

This field is totally real and has an integral basis

$$\{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7, \xi^8, \omega_{10}, \omega_{11}, \omega_{12}\}$$

with

$$\begin{aligned} \omega_{10} &= (1 + \xi^3 + 2\xi^4 + \xi^6 + \xi^7 + \xi^8 + \xi^9)/3 \\ \omega_{11} &= (2 + \xi + 2\xi^3 + 2\xi^4 + 2\xi^5 + 2\xi^6\xi^{10})/3 \\ \omega_{12} &= (107761264539 + 9245049222\xi + 31097752879\xi^2 + 40137945519\xi^3 \\ &\quad + 34157911107\xi^4 + 93111405784\xi^5 + 51616938926\xi^6 \\ &\quad + 54389034027\xi^7 + 110416671757\xi^8 + 1812369088\xi^9 \\ &\quad + 25415148001\xi^{10} + \xi^{11})/113333753409. \end{aligned}$$

The field K has a totally real quartic subfield L generated by α defined by the polynomial $g(x) = x^4 - 4x^2 + x + 1$. (Note that K has also a cubic subfield generated by the root of $x^3 + 4x^2 - 2x - 1$ but this is not interesting in our arguments.) The field L has integral basis $\{1, \alpha, \alpha^2, \alpha^3\}$ and fundamental units

$$\eta_1 = \alpha, \quad \eta_2 = 1 - \alpha, \quad \eta_3 = -2\alpha + \alpha^2 + \alpha^3.$$

The units η_1, η_2, $\eta_3, \varepsilon_1, \dots, \varepsilon_8$ form a system of fundamental units in K, where the coefficients of $\varepsilon_1, \dots, \varepsilon_8$ in the integral basis of K are the following:

$$\begin{aligned} \varepsilon_1 = [&-10895130684, 3196295645, -6147000968, 2471771060, 4012072493, \\ &-8357582270, 202752252, -10392673880, -21467491622, \\ &-1074736976, -15071211644, 22402348184] \end{aligned}$$

$$\begin{aligned}\varepsilon_2 = [&761572045, -223421774, 429676837, -172777352, -280445134,\\ &584196946, -14172204, 726450169, 1500582390, 75124353,\\ &1053481036, -1565929104]\end{aligned}$$

$$\begin{aligned}\varepsilon_3 = [&97534039010, -28613481877, 55028420322, -22127482530,\\ &-35916377883, 74817712333, -1815053823, 93036007507,\\ &192178618710, 9621127196, 134918633553, -200547525759]\end{aligned}$$

$$\begin{aligned}\varepsilon_4 = [&53135222443, -15588237092, 29978737346, -12054752441,\\ &-19566755165, 40759675309, -988817143, 50684755933,\\ &104696306673, 5241459687, 73501842816, -109255573732]\end{aligned}$$

$$\begin{aligned}\varepsilon_5 = [&-137633535407, 40377438576, -77652439063, 31224828557,\\ &50682797994, -105577768977, 2561283431, -131286213220,\\ &-271189658479, -13576693470, -190388183616, 282999302268]\end{aligned}$$

$$\begin{aligned}\varepsilon_6 = [&22062864796, -6472564754, 12447804013, -5005387339,\\ &-8124529892, 16924276765, -410577392, 21045379385,\\ &43472114179, 2176364587, 30519515049, -45365218051]\end{aligned}$$

$$\begin{aligned}\varepsilon_7 = [&-62200893641, 18247825609, -35093562605, 14111475601,\\ &22905139427, -47713891702, 1157523982, -59332340433,\\ &-122559077246, -6135731847, -86042366935, 127896224154]\end{aligned}$$

$$\begin{aligned}\varepsilon_8 = [&465526096893, -136571013123, 262648465963, -105613596395,\\ &-171427445547, 357101971563, -8663180146, 444057171072,\\ &917260919255, 45921258230, 643961282807, -957205380390]\end{aligned}$$

Hence $s = 3$, $r = 8, q = 1$.

Consider the norm form equation

$$\begin{aligned} &N_{K/\mathbb{Q}}(x_1 + \alpha x_2 + \alpha^2 x_3 + \alpha^3 x_4 + \xi x_5) = \pm 1 \\ &\text{in } x_1, x_2, x_3, x_4, x_5 \in \mathbb{Z} \quad \text{with } x_5 \neq 0. \end{aligned} \tag{24}$$

We had $c_1 = 0.5187$ and $c_2 = 3.9495$ for all possible i, j_1, j_2. Since our example is a totally real one, we did not have to use a_0. Baker's method gave

$$A = \max(|a_1|, \dots, |a_8|) \leq 10^{46} = A_B.$$

In the reduction procedure we had dimension 9, $c_3 = 1/c_1$, $c_4 = 0$. The following table summarizes the steps of the reduction procedure. Note that in each step we had to perform 12 reductions.

	$A <$	$\|b_1\| >$	$H =$	precision	bound for A	CPU time
Step I	10^{46}	10^{48}	10^{440}	1100 digits	472	98 min
Step II	472	23884	10^{40}	100 digits	45	60 sec
Step III	45	2277	10^{35}	80 digits	40	60 sec
Step IV	40	2024	10^{30}	80 digits	34	60 sec

Hence our algorithm gave the reduced bound $A_R = 34$.

In the enumeration process we used

$$I^* = \{(i123), (i231), (i312) \mid i = 1, 2, 3, 4\}$$

that is we had $t = 12$ ellipsoids to consider. The initial bound was $S = 0.128 \cdot 10^{174}$ that we got using the reduced bound for A. Note that also in this example the vector $\underline{g}$ is linearly dependent on $\underline{e}_1, \ldots, \underline{e}_8$. The following table is a summary of the enumeration process.

	S	s	precision	CPU time	tuples found
Step I	10^{174}	10^{20}	100 digits	15 sec	0
Step II	10^{20}	10^{10}	50 digits	10 sec	2
Step III	10^{10}	10^{8}	50 digits	10 sec	2
Step IV	10^{8}	10^{6}	50 digits	8 sec	24
Step V	10^{6}	10^{5}	50 digits	5 sec	26
Step VI	10^{5}	10^{4}	50 digits	15 sec	91
Step VII	10^{4}	10^{3}	50 digits	15 sec	178
Step VIII	1000	500	50 digits	15 sec	57
Step IX	500	250	50 digits	10 sec	45
Step X	250	120	50 digits	10 sec	37
Step XI	120	60	50 digits	12 sec	60
Step XII	60	30	50 digits	10 sec	24
Step XIII	30	15	50 digits	10 sec	17
Step XIV	15	7	50 digits	10 sec	18
Step XV	7	4	50 digits	10 sec	16
Step XVI	4		50 digits	3 sec	125

The last line refers to the enumeration of the ellipsoid (19) with $s = 4$.

We tested all tuples we found in the enumeration process if they are solutions of (4). We found 5 solutions of (4), the components were all ≤ 1 in absolute value. For these tuples we calculated the corresponding solutions of the equation (23). We obtained the following solutions:

x_1	x_2	x_3	x_4	x_5
-2	4	0	-1	-1
1	3	0	-1	1
0	1	-1	0	1
0	0	0	0	1

If $(x_1, x_2, x_3, x_4, x_5)$ is a solution then so also is $(-x_1, -x_2, -x_3, -x_4, -x_5)$ but we list only one of them.

References

[1] A. Baker and G. Wüstholz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993), 19–62.

[2] Y. Bilu and G. Hanrot, Solving Thue equations of high degree, *J. Number Theory* **60** (1996), 373–392.

[3] Y. Bugeaud and K. Győry, Bounds for the solutions of Thue–Mahler equations and norm form equations, *Acta Arith.* **74** (1996), 273–292.

[4] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roeger, M. Schörnig and K. Wildanger, *KANT V4, J. Symbolic Comput.* **24** (1997), 267–283.

[5] U. Fincke and M. Pohst, Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, *Math. Comp.* **44** (1985), 463–471.

[6] I. Gaál, Power integral bases in algebraic number fields, in: Number Theory (K. Győry, A. Pethő, V. T. Sós, eds.), *Walter de Gruyter*, 1988, 243–254.

[7] I. Gaál, Power integral bases in algebraic number fields II., Proc. Conf. Graz, 1988, *Walter de Gruyter* (*to appear*).

[8] I. Gaál and M. Pohst, On the resolution of relative Thue equations (*to appear*).

[9] K. Győry, On the representation of integers by decomposable forms in several variables, *Publ. Math. Debrecen* **28** (1981), 89–98.

[10] A. Pethő and R. Schulenberg, Effektives lösen von Thue Gleichungen, *Publ. Math. Debrecen* **34** (1987), 189–196.

[11] N. P. Smart, The solution of trigangularly connected decomposable form equations, *Math. Comput.* **64** (1995), 819–840.

[12] N. P. Smart, Thue and Thue–Mahler equations over rings of integers, *J. London Math. Soc.* **56** no. 2 (1997), 455–462.

[13] N. Tzanakis and B. M. M. de Weger, On the practical solution of the Thue equation, *J. Number Theory* **31** (1989), 99–132.

[14] K. Wildanger, Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve, Dissertation, *Technical University*, *Berlin*, 1997.

ISTVÁN GAÁL
MATHEMATICAL INSTITUTE
UNIVERSITY OF DEBRECEN
H–4010 DEBRECEN P.O. BOX 12
HUNGARY

E-mail: igaal@math.klte.hu

(Received May 28, 1999)