

# Computing small solutions of unit equations in three variables I: Application to norm form equations

István Járasi  
University of Debrecen,  
Institute of Mathematics  
H-4010 Debrecen Pf.12  
e-mail: [ijarasi@math.klte.hu](mailto:ijarasi@math.klte.hu) \*

## Abstract

We construct an algorithm to enumerate small solutions of unit equations in three variables. The algorithm is a generalization of K.Wildanger's method [17] and of the method of I.Gaál and M.Pohst [6], and is based on the method of U.Fincke and M.Pohst [4] enumerating lattice points in ellipsoids (see also I.Gaál [5]).

We will call a solution small if it has "small" exponents corresponding to a given system of fundamental units. Our method can be applied also in the case when the unknown units are composed of some independent units. We demonstrate our method by enumerating small solutions of a norm form equation, with four unknown exponents involved with absolute values less than  $A = 200$ .

## 1 Introduction

In the 1960's A.Baker established the effective theory of diophantine equations in two unknowns like Thue equations. In 1969 A.Baker and H.Davenport [1] opened a new horizon: the constructive algorithmic theory of diophantine equations by their reduction method. Here we cite some results of this new area corresponding to our paper.

In 1987 A.Pethó [14] has developed a fast algorithm for finding small solutions of Thue equations. N.Tzanakis and B.M.M. de Weger [16], A.Pethó and R.Schulenberg [15] developed algorithm for the complete resolution of Thue equations. They found that usually there are only small solutions of Thue equations. Y.Bilu and G.Hanrot [2] has completed the algorithmic approach to Thue equations.

---

\*2000 Mathematics Subject Classification: 11Y50, 11D57, key words and phrases: unit equations, norm form equations

More generally K.Györy (see e.g. [9],[11]) investigated decomposable form equations, which contain as special cases Thue equations, norm form, discriminant form, index form and resultant form equations. General discriminant form and index form equations and a large class of norm form equations (including Thue equations) were reduced by K.Györy to unit equations in two variables of type

$$\alpha_1 u_1 + \alpha_2 u_2 = 1$$

(in the unknown units  $u_1, u_2$ ) for which he applied ([7],[8]) Baker's method to derive upper bounds for the solutions. Applying reduction methods and enumeration processes due to K.Wildanger recently it became possible to solve some of these equations completely (see [5]). These equations usually only have "small" solutions. These methods are described in the monograph I.Gaál [5].

J.-H.Evertse, K.Györy and C.Stewart (see e.g. [3]) showed that arbitrary decomposable form equations are equivalent to a system of unit equations in *several variables*.

Baker's method could not be applied to unit equations in more than two variables, so there is no hope to solve these equations completely.

We are going to give an algorithm for calculating "small" solutions of unit equations in three variables. The application of this method makes possible to find "small" solutions of some classes of decomposable form equations, that formerly could not be dealt with by using the above standard tools. The method is based on the ideas of K.Wildanger [17] and I.Gaál and M.Pohst [6] (see also [5]) and uses the method of U.Fincke and M.Pohst [4] for enumerating points in ellipsoids.

In the present paper we shall apply the method to certain norm form equations. In a forthcoming paper we shall investigate resultant type equations.

## 2 Preliminary definitions and results

### 2.1 Semi-orbits, enumerable semi-orbits

Let  $x, y \in \mathbb{C}^*$ . The set

$$\mathfrak{D}(x, y) = \left\{ x, \frac{1}{x}, y, \frac{1}{y}, -\frac{x}{y}, -\frac{y}{x} \right\}$$

will be called the *semi-orbit* of  $x$  and  $y$ . The elements  $x$  and  $y$  are the generators of the semi-orbit  $\mathfrak{D}(x, y)$ .

One can see that if  $x = \varepsilon$  is an exceptional unit ( $\varepsilon$  and  $1 - \varepsilon$  are both units, a definition due to Nagell) of an algebraic number field, then

$$\mathfrak{D}(\varepsilon, 1 - \varepsilon) = \Omega(\varepsilon)$$

where  $\Omega(\varepsilon)$  is the orbit of  $\varepsilon$ , that is

$$\Omega(\varepsilon) = \left\{ \varepsilon, 1 - \varepsilon, \frac{1}{\varepsilon}, \frac{1}{1 - \varepsilon}, \frac{\varepsilon}{\varepsilon - 1}, \frac{\varepsilon - 1}{\varepsilon} \right\}$$

in the terminology of K.Wildanger [17].

We will call a semi-orbit  $\mathfrak{D}(x, y)$  *enumerable* if for all  $u \in \mathfrak{D}(x, y)$  there is a  $v \in \mathfrak{D}(x, y)$  such that

$$|u + v| \leq 2 \quad \text{and} \quad \frac{u}{v} \in \mathfrak{D}(x, y)$$

We will denote it by  $\mathfrak{D}^2(x, y)$ .

**Lemma 1.** *Let  $x_1, x_2, x_3 \in \mathbb{C}^*$  and*

$$M_0(x_1, x_2, x_3) = \{x_1, x_2, x_3\} \quad M_1(x_1, x_2, x_3) = \left\{ \frac{1}{x_1}, -\frac{x_2}{x_1}, -\frac{x_3}{x_1} \right\}$$

$$M_2(x_1, x_2, x_3) = \left\{ \frac{1}{x_2}, -\frac{x_1}{x_2}, -\frac{x_3}{x_2} \right\} \quad M_3(x_1, x_2, x_3) = \left\{ \frac{1}{x_3}, -\frac{x_1}{x_3}, -\frac{x_2}{x_3} \right\}$$

Then

$$\max_{i=0, \dots, 3} (\min(M_i^{\parallel}(x_1, x_2, x_3))) \geq 1$$

where  $M^{\parallel}$  consists of the absolute values of the elements of  $M$  and  $\min(M^{\parallel})$  is the minimum of the set  $M^{\parallel}$ .

*Proof.* Using symmetry considerations we have the following four cases:

1.

$$|x_1| \geq 1 \quad |x_2| \geq 1 \quad |x_3| \geq 1$$

This implies  $\min M_0^{\parallel}(x_1, x_2, x_3) \geq 1$ .

2.

$$|x_1| \geq 1 \quad |x_2| \geq 1 \quad |x_3| \leq 1$$

In this case one can check that  $\min M_3^{\parallel}(x_1, x_2, x_3) \geq 1$ .

3.

$$|x_1| \geq 1 \quad |x_2| \leq 1 \quad |x_3| \leq 1$$

In this case we may also assume that  $|x_3| \geq |x_2|$ . Using this it is easy to see that  $\min M_2^{\parallel}(x_1, x_2, x_3) \geq 1$ .

4.

$$|x_1| \leq 1 \quad |x_2| \leq 1 \quad |x_3| \leq 1$$

In this case one can also assume that  $x_1$  has the least absolute value. Then  $\min M_1^{\parallel}(x_1, x_2, x_3) \geq 1$ .

□

**Corollary 1.** Let  $x_1, x_2, x_3 \in \mathbb{C}^*$  be such that

$$x_1 + x_2 + x_3 = 1.$$

Then there are  $i \in \{0, \dots, 3\}$  and  $u, v \in M_i(x_1, x_2, x_3)$  such that  $\mathfrak{D}(u, v)$  is enumerable.

*Proof.* Use the previous lemma for  $x_1, x_2, x_3$ . Using symmetry considerations, we may also assume that  $\min M_1^{\parallel}(x_1, x_2, x_3) \geq 1$ . This also means that  $\max(\frac{1}{|x_1|}, \frac{1}{|x_2|}, \frac{1}{|x_3|}) \leq 1$  which yields

$$\begin{aligned} \left| -\frac{x_2}{x_1} - \frac{x_3}{x_1} \right| &= \left| 1 - \frac{1}{x_1} \right| \leq 2 \\ \left| -\frac{x_1}{x_2} - \frac{x_3}{x_2} \right| &= \left| 1 - \frac{1}{x_2} \right| \leq 2 \\ \left| -\frac{x_1}{x_3} - \frac{x_2}{x_3} \right| &= \left| 1 - \frac{1}{x_3} \right| \leq 2 \end{aligned}$$

Using these equations one can see that if  $u = -\frac{x_2}{x_1}$  and  $v = -\frac{x_3}{x_1}$  then  $\mathfrak{D} = \mathfrak{D}(u, v)$  is enumerable, since for every element of  $\mathfrak{D}$  the desired other element is the one appearing in the same equation listed above.  $\square$

**Remark.** Using the above Corollary one can choose  $\binom{3}{2} = 3$  such pairs of  $(u, v)$ -s from the four  $M_i$ -s. This means  $3 \cdot 4 = 12$  pairs. In fact by

$$\mathfrak{D}(u, v) = \mathfrak{D}\left(\frac{1}{u}, -\frac{v}{u}\right) = \mathfrak{D}\left(\frac{1}{v}, -\frac{u}{v}\right)$$

we have only four possible pairs of  $(u, v)$  that generates pairwise different semi-orbits. These four pairs will be called the *primitive pairs* of  $(x_1, x_2, x_3)$ .

## 2.2 Reduction of enumerable semi-orbits

**Lemma 2.** Let  $x, y \in \mathbb{C}^*$ , and let  $S > s > 2$  be positive real numbers such that for all  $z \in \mathfrak{D}^2(x, y)$

$$\frac{1}{S} \leq |z| \leq S.$$

Then

1. either for all  $z \in \mathfrak{D}^2(x, y)$  we have

$$\frac{1}{s} \leq |z| \leq s$$

2. or there is a  $z \in \mathfrak{D}^2(x, y)$  such that

$$|\log |z|| \leq \frac{2}{s-2}$$

*Proof.* Suppose that the first case does not hold. Then there is an  $u \in \mathfrak{D}^2(x, y)$  such that

$$s \leq |u| \leq S.$$

We also have a  $v$  in  $\mathfrak{D}^2(x, y)$  such that

$$\left| |u| - |v| \right| \leq |u + v| \leq 2 \quad \text{and} \quad \frac{u}{v} \in \mathfrak{D}^2(x, y)$$

By  $s \leq |u|$  we also have

$$\min(|u|, |v|) \geq s - 2$$

and using Lagrange's Mean Value Theorem we conclude

$$\left| \log \frac{|u|}{|v|} \right| = \left| \log |u| - \log |v| \right| \leq \frac{1}{\min(|u|, |v|)} \left| |u| - |v| \right| \leq \frac{2}{s - 2}.$$

Observe that  $\frac{u}{v}$  is also in  $\mathfrak{D}^2(x, y)$  so the second case of the statement of the lemma is satisfied with  $z = \frac{u}{v}$ .  $\square$

Obviously the notion of enumerable semi-orbit  $\mathfrak{D}^2(x, y)$  is based on this lemma.

### 3 Unit equations in three variables

Let  $K$  be an algebraic number field of degree  $[K : \mathbb{Q}] = d > 3$ . In the following we construct a method to determine the "small" solutions of the unit equation of type

$$u^{(1)} + u^{(2)} + u^{(3)} + u^{(4)} = 0 \tag{1}$$

where (and in the following)  $u^{(i)}$  denotes the  $i$ -th conjugate of a unit  $u \in K$ . The diophantine equations we consider in Section 5 lead in fact to this special type of unit equations (written in a homogeneous form). Without significant changes our method can also be applied to general unit equations of the form

$$a_1 u^{(1)} + a_2 u^{(2)} + a_3 u^{(3)} + a_4 u^{(4)} = 0 \tag{2}$$

where the  $a_i$ -s are given elements in  $\overline{K}$  (the normal closure of  $K$ ).

Obviously, equation (1) can be written in the following four equivalent inhomogeneous forms:

$$\begin{aligned} -\frac{u^{(2)}}{u^{(1)}} - \frac{u^{(3)}}{u^{(1)}} - \frac{u^{(4)}}{u^{(1)}} &= 1 \\ -\frac{u^{(1)}}{u^{(2)}} - \frac{u^{(3)}}{u^{(2)}} - \frac{u^{(4)}}{u^{(2)}} &= 1 \\ -\frac{u^{(1)}}{u^{(3)}} - \frac{u^{(2)}}{u^{(3)}} - \frac{u^{(4)}}{u^{(3)}} &= 1 \\ -\frac{u^{(1)}}{u^{(4)}} - \frac{u^{(2)}}{u^{(4)}} - \frac{u^{(3)}}{u^{(4)}} &= 1 \end{aligned}$$

These are indeed special forms of *unit equations* in three variables.

Several types of decomposable form equations can be reduced to unit equations in three variables, for example norm form equations in three unknowns, resultant form equations. In Section 5 we detail an application of our method to norm form equations. For the application to resultant form equations see [13].

## 4 The enumeration method

Let  $r$  be the unit rank of  $K$ , and let  $\varepsilon_i$ ,  $i = 1, \dots, r$  be fundamental units of  $K$ . It is important to remark that we do not really need the fundamental units. Without significant changes our method can be applied to a system of  $r$  independent units. See the corresponding paper of G.Hanrot [12].

Let  $\mathfrak{D}$  be a set containing some nontrivial quotients of the units in equation (1), that is

$$\mathfrak{D} = \left\{ \frac{u^{(i)}}{u^{(j)}} \mid (i, j) \in \Gamma_{\mathfrak{D}} \right\}$$

where  $\Gamma_{\mathfrak{D}} = \{(i_l, j_l) \mid l = 1, \dots, g\}$  is a suitable index set. We shall call  $\Gamma_{\mathfrak{D}}$  the *index set* corresponding to  $\mathfrak{D}$ . If such an  $\mathfrak{D}$  is a union of semi-orbits then it will be called an *enumerable set*.

In the enumeration method we will need the following

**Definition 1.** Let  $\mathfrak{D}$  be an enumerable set with corresponding index set  $\Gamma_{\mathfrak{D}} = \{(i_l, j_l) \mid l = 1, \dots, g\}$ . By the rank of  $\mathfrak{D}$  we mean the dimension of the vector space spanned by the vectors

$$\underline{e}_k = \begin{pmatrix} \log \left| \frac{\varepsilon_k^{(i_1)}}{\varepsilon_k^{(j_1)}} \right| \\ \vdots \\ \log \left| \frac{\varepsilon_k^{(i_g)}}{\varepsilon_k^{(j_g)}} \right| \end{pmatrix} \text{ for } k = 1, \dots, r.$$

In fact the rank of such an enumerable set can be determined exactly. Let  $\Gamma_{\mathfrak{D}} = \{(i_l, j_l) \mid l = 1, \dots, g\}$  be the corresponding index set. Let  $R$  be the regulator matrix of  $K$  i.e.  $R_{ij} = \log |\varepsilon_j^{(i)}|$ . Let  $T$  be the matrix in which the  $l$ -th row contains 1 at the  $i_l$ -th place and  $-1$  at  $j_l$ -th place, and the others are zeros for  $l = 1, \dots, g$ . Then the matrix-product  $T \cdot R$  contains the vectors  $\underline{e}_k$  as columns. Since the rank of  $R$  is the unit rank of  $K$  (so  $R$  has maximal rank) and the rank of  $T$  can be computed using integer arithmetic, the rank of  $T \cdot R$  so the rank of the enumerable set can be computed explicitly, it will be the rank of  $T$ . In our numerical examples we used this method to compute the ranks.

## 4.1 Localizing the solutions of unit equations in three variables

The basic idea of the enumeration method was settled by K.Wildanger [17]. These ideas were further developed to the case of conjugate units by I.Gaál and M.Pohst [6], see also [5]. Here we extend these ideas to our case of unit equations in three variables.

**Theorem 1.** *For every unit equation in three variables of type (1) and every  $g \in \{1, \dots, d\}$  there are enumerable sets  $\mathfrak{D}_1, \dots, \mathfrak{D}_{4^g}$  such that if  $u$  is a solution of (1) then there is an  $i \in \{1, \dots, 4^g\}$  and  $g$  triples of indices  $(j_m, k_m, l_m)$  for  $m = 1, \dots, g$  with*

$$\mathfrak{D}_i = \bigcup_{m=1}^g \mathfrak{D}^2\left(-\frac{u^{(j_m)}}{u^{(l_m)}}, -\frac{u^{(k_m)}}{u^{(l_m)}}\right)$$

*Proof.* Suppose that  $u$  is a solution of (1). To construct the enumerable sets choose some conjugates of (1), say the first  $g$  of them, where  $1 \leq g \leq d$ . Using the equivalent forms of this equation (see Section 3) one can apply Corollary 1 to the tuples

$$\left(-\frac{(u^{(2)})^{(i)}}{(u^{(1)})^{(i)}}, -\frac{(u^{(3)})^{(i)}}{(u^{(1)})^{(i)}}, -\frac{(u^{(4)})^{(i)}}{(u^{(1)})^{(i)}}\right)$$

for  $i = 1, \dots, g$  where  $(u^{(j)})^{(i)}$  is the image of  $u^{(j)}$  under the Galois action of the normal closure of  $K$  which sends  $u^{(1)}$  to  $u^{(i)}$ . For every tuple we have 4 possible primitive pairs

$$(v_{i_1}, w_{i_1}), (v_{i_2}, w_{i_2}), (v_{i_3}, w_{i_3}), (v_{i_4}, w_{i_4})$$

for  $i = 1, \dots, g$ . Now construct the  $4^g$  enumerable sets by building the union of the semi-orbits generated by one of the four primitive pairs for every  $i = 1, \dots, g$ . Let these be  $\mathfrak{D}_1, \dots, \mathfrak{D}_{4^g}$ .

Since  $u$  is a solution of (1), for every  $i = 1, \dots, g$  there is a primitive pair  $(u_{j_i}, v_{j_i})$  such that  $\mathfrak{D}(u_{j_i}, v_{j_i})$  is enumerable, so the enumerable set constructed with these primitive pairs is suitable.  $\square$

**Remark:** In the above Theorem  $g$  is arbitrary with  $1 \leq g \leq d$ . It is even possible to choose  $g = 1$ , but in that case it is too complicated to enumerate the possible solutions. Taking  $g = d$  it is the easiest to enumerate the solutions in the enumerable sets, but then there are too many solutions. Therefore we have to make a compromise in choosing  $g$ .

This Theorem localizes all (!) solutions of unit equations in three unknowns in finite number of enumerable sets. Equivalently: it is enough to deal with enumerable sets. Since there are no effective upper bounds on the heights of the solutions, there is no hope to determine all solutions in practice. Our purpose is to calculate the "small" solutions with

$$A \leq A_0$$

where  $A_0 > 0$  is given, and  $A = \max(|a_1|, \dots, |a_r|)$ , using the representation

$$\log |u^{(i)}| = a_1 \log |\varepsilon_1^{(i)}| + \dots + a_r \log |\varepsilon_r^{(i)}|.$$

We note that this bound on the absolute values of the exponents can be translated to a bound on the absolute values of the  $u_i$ -s and conversely. In our example  $A_0 = 200$  which is a usual bound solving practically unit equations in two unknowns. In fact these "small" solutions usually cover all solutions (the experiments show that such equations only have "small" solutions) but we do not prove that indeed there are no "large" ones.

## 4.2 The enumeration lemma and its application

**Lemma 3.** *Let  $S > s > 2$  be positive numbers. Let  $\mathfrak{D}$  be an enumerable set which is the union of enumerable semi-orbits. Suppose that for every  $u \in \mathfrak{D}$  we have*

$$\frac{1}{S} \leq |u| \leq S$$

Then

1. either for all  $u \in \mathfrak{D}$

$$\frac{1}{s} \leq |u| \leq s$$

2. or there is a  $u \in \mathfrak{D}$  such that

$$|\log |u|| \leq \frac{2}{s-2}$$

*Proof.* Since  $\mathfrak{D}$  is the union of enumerable semi-orbits, one can use Lemma 2.  $\square$

This lemma can be applied in the following way (we detail only the totally real case, the complex case is similar):

Let  $S_0 > S_1 > \dots > S_m > 2$  be a sequence of positive numbers such that

$$\frac{1}{S_0} \leq \left| \frac{u^{(i)}}{u^{(j)}} \right| \leq S_0 \quad \text{for all possible } i, j.$$

Such an  $S_0$  can be determined by

$$\log S_0 = A_0 \max \left( \left| \log \left| \frac{\varepsilon_1^{(i)}}{\varepsilon_1^{(j)}} \right| \right| + \dots + \left| \log \left| \frac{\varepsilon_r^{(i)}}{\varepsilon_r^{(j)}} \right| \right| \right), \quad (3)$$

where  $A_0$  is the maximum of the exponents mentioned above.

The constant  $S_{n-1}$  can be replaced by the smaller constant  $S_n$  if for each  $(i_0, j_0) \in \Gamma_{\mathfrak{D}}$  we enumerate directly the set  $H_{i_0 j_0}$  of those exponent vectors  $(a_1, \dots, a_r)$  for which

$$\frac{1}{S_{n-1}} \leq \left| \frac{u_i}{u_j} \right| \leq S_{n-1} \text{ for all } (i, j) \in \Gamma_{\mathfrak{D}} \text{ and } \left| \log \left| \frac{u_{i_0}}{u_{j_0}} \right| \right| \leq \frac{2}{S_n - 2}.$$

We show that such exponent vectors are contained in an ellipsoid. To enumerate the points of this ellipsoid we use the algorithm of U.Fincke and M.Pohst [4]. The application of this lemma is similar as in [6], see also [5].

In order to be able to use the above lemma, the union of a  $d$ -tuple of enumerable semi-orbits has to have full rank. Note that since this union is an enumerable set, it has a well defined rank, see the beginning of Section 4. In our example we always found  $d$ -tuples with rank less than  $r$ . In that case one has to add some more  $-\frac{u^{(i')}}{u^{(j')}}$  to  $\mathfrak{D}$  to make its rank full. These will be called *additional elements*. For details see the numerical results in Section 5.2.

For this purpose let  $\mathfrak{D}'$  be the set of additional elements such that  $\mathfrak{D} \cup \mathfrak{D}'$  has full rank. Denote by  $\Gamma_{\mathfrak{D} \cup \mathfrak{D}'} = \{(i_1, j_1), \dots, (i_t, j_t)\}$  the index set corresponding to  $\mathfrak{D} \cup \mathfrak{D}'$  and let  $(i_0, j_0)$  be a fixed pair in  $\Gamma_{\mathfrak{D}}$ . Further let

$$\underline{e}_h = \begin{pmatrix} \log \left| \frac{\varepsilon_h^{(i_1)}}{\varepsilon_h^{(j_1)}} \right| \\ \vdots \\ \log \left| \frac{\varepsilon_h^{(i_t)}}{\varepsilon_h^{(j_t)}} \right| \end{pmatrix} \text{ for } h = 1, \dots, r,$$

$$\lambda_p = \begin{cases} \frac{1}{\log S_{n-1}} & \text{for } (i_p, j_p) \neq (i_0, j_0) \text{ but } (i_p, j_p) \in \Gamma_{\mathfrak{D}} \\ \frac{S_n - 2}{2} & \text{for } (i_p, j_p) \neq (i_0, j_0) \\ \frac{1}{\log S_0} & \text{for } (i_p, j_p) \in \Gamma_{\mathfrak{D}'} \end{cases}$$

$$\phi_{i_0 j_0}(\underline{b}) = \begin{pmatrix} \lambda_1 \log \left| \frac{u^{(i_1)}}{u^{(j_1)}} \right| \\ \vdots \\ \lambda_t \log \left| \frac{u^{(i_t)}}{u^{(j_t)}} \right| \end{pmatrix}$$

and

$$\phi_{i_0 j_0}(\underline{e}_k) = \begin{pmatrix} \lambda_1 \log \left| \frac{\varepsilon_k^{(i_1)}}{\varepsilon_k^{(j_1)}} \right| \\ \vdots \\ \lambda_t \log \left| \frac{\varepsilon_k^{(i_t)}}{\varepsilon_k^{(j_t)}} \right| \end{pmatrix} \text{ for } k = 1, \dots, r$$

Since  $\underline{e}_1, \dots, \underline{e}_r$  are linearly independent, so are their images. So we have

$$\phi_{i_0 j_0}(\underline{b}) = a_1 \phi_{i_0 j_0}(\underline{e}_1) + \dots + a_r \phi_{i_0 j_0}(\underline{e}_r).$$

Moreover we become

$$\begin{aligned} |a_1 \phi_{i_0 j_0}(\underline{e}_1) + \dots + a_r \phi_{i_0 j_0}(\underline{e}_r)|^2 &= |\phi_{i_0 j_0}(\underline{b})|^2 = \\ &= \sum_{p=0}^t \lambda_p^2 \log^2 \left| \frac{u^{(i_p)}}{u^{(j_p)}} \right| \leq t \end{aligned}$$

which means that the  $(a_1, \dots, a_r)$  are contained in an ellipsoid which we can enumerate by the method of U.Fincke and M.Pohst [4].

After this we have to consider the smallest solutions, for which

$$\frac{1}{3} \leq \left| \frac{u^{(i)}}{u^{(j)}} \right| \leq 3 \text{ for all } (i, j) \in \Gamma_{\mathfrak{D}}$$

In this case there are two possibilities:

- 1 The set  $\mathfrak{D}$  has full rank, then the corresponding exponent vectors can be covered by an ellipsoid, for details see [17],[5].
- 2 The set  $\mathfrak{D}$  has rank  $r_1 < r$ , then one should choose a generating subset of the vectors  $\{\underline{e}_i | i = 1, \dots, r\}$  (here the  $\underline{e}_i$ -s have coordinates corresponding only to  $\mathfrak{D}$ ). Suppose that the first  $r_1$  vectors are linearly independent. This means that there are  $\mu_{kl} \in \mathbb{R}$  such that

$$\underline{e}_{r_1+i} = \mu_{i1}\underline{e}_1 + \dots + \mu_{ir_1}\underline{e}_{r_1} \quad \text{for } i = 1, \dots, r - r_1$$

so for every  $(a_{r_1+1}, \dots, a_r) \in ([-A, A] \cap \mathbb{Z})^{r-r_1}$  the vector

$$a_{r_1+1}\underline{e}_{r_1+1} + \dots + a_r\underline{e}_r$$

is a linear combination of the vectors  $\underline{e}_1, \dots, \underline{e}_{r_1}$ . Then for every fixed  $(a_{r_1+1}, \dots, a_r) \in ([-A, A] \cap \mathbb{Z})^{r-r_1}$  one has to construct the ellipsoids using the vectors

$$a_1\underline{e}_1 + \dots + a_{r_1}\underline{e}_{r_1} + a_{r_1+1}\underline{e}_{r_1+1} + \dots + a_r\underline{e}_r$$

which will define ellipsoids containing only the exponent vectors  $(a_1, \dots, a_{r_1})$ .

## 5 Application to norm form equation

### 5.1 Norm form equations in three unknowns

In the following we use the results of the previous sections to enumerate the "small" solutions of a given norm form equation in three variables.

Let  $K = \mathbb{Q}(\alpha)$  be a totally real quintic number field, and let  $\alpha \in \mathbb{Z}_K$ . In the following we would like to determine the small solutions of the equation

$$N_{K/\mathbb{Q}}(x_1 + \alpha x_2 + \alpha^2 x_3) = \pm 1$$

in the integer unknowns  $x_1, x_2, x_3$ . We note that one can substitute  $\pm 1$  by any given integer  $m \neq 0$  and can use our method without significant changes.

For any  $\gamma \in K$  denote by  $\gamma^{(i)}$  its conjugate for  $i = 1, \dots, 5$ . Then

$$N_{K/\mathbb{Q}}(x_1 + \alpha x_2 + \alpha^2 x_3) = \prod_{i=1}^5 (x_1 + \alpha^{(i)} x_2 + (\alpha^{(i)})^2 x_3)$$

holds. Using this we can write

$$x_1 + \alpha^{(i)}x_2 + (\alpha^{(i)})^2x_3 = \pm \left(\varepsilon_1^{(i)}\right)^{a_1} \cdot \dots \cdot \left(\varepsilon_4^{(i)}\right)^{a_4} \quad (4)$$

where  $\varepsilon_1, \dots, \varepsilon_4$  are the fundamental units of  $K$ , the  $a_k$ -s are in  $\mathbb{Z}$ .

Let  $i, j, k, l$  be four distinct indices from the index set  $\{1, 2, 3, 4, 5\}$  such that  $i \leq j \leq k \leq l$ . Let

$$u^{(i)} = \prod_{p=1}^4 (\varepsilon_p^{(i)})^{a_p},$$

and

$$|1, \alpha, \alpha^2|^{(jkl)} = \begin{vmatrix} 1 & \alpha^{(j)} & (\alpha^{(j)})^2 \\ 1 & \alpha^{(k)} & (\alpha^{(k)})^2 \\ 1 & \alpha^{(l)} & (\alpha^{(l)})^2 \end{vmatrix}.$$

Then using standard arguments one has

$$u^{(i)}|1, \alpha, \alpha^2|^{(jkl)} - u^{(j)}|1, \alpha, \alpha^2|^{(ikl)} + u^{(k)}|1, \alpha, \alpha^2|^{(ijl)} - u^{(l)}|1, \alpha, \alpha^2|^{(ijk)} = 0 \quad (5)$$

and to this equation we use our method with  $A = \max_{i=1, \dots, 4} (|a_i|) \leq A_0 = 200$ .

We note that if one would try all the  $(2 \cdot 200 + 1)^4 = 25856961601 \approx 2.6 \cdot 10^{10}$  possibilities for the exponent vectors, then the test would take about 2600 days on the same machine we have used.

## 5.2 A numerical example

Let  $K$  be generated by a root  $\alpha$  of  $x^5 - 5x^3 + x^2 + 3x - 1$ . This is a totally real quintic field with unit rank 4. Consider the equation

$$N_{K/\mathbb{Q}}(x + y\alpha + z\alpha^2) = \pm 1. \quad (6)$$

Using our method we have enumerated all solutions of (6) with

$$X = \max(|x|, |y|, |z|) \leq 10^{10}. \quad (7)$$

Using standard tools one can see that this set is covered by the

$$A = \max(|a_1|, |a_2|, |a_3|, |a_4|) \leq A_0 = 200$$

where the  $a_i$ -s correspond to the representation (4).

We have used 2 of the 5 conjugates of the unit equation (5) so we had to perform  $4^2 = 16$  reduction and enumeration processes.

In six of the processes the set  $\mathfrak{D}$  (the union of the enumerable semi-orbits) had rank 4, so we did not need any additional terms. In these cases the CPU time was quite short, about 2 minutes on a Celeron 800 Mhz processor.

In nine of the processes the set  $\mathfrak{D}$  had rank 3, so we had to choose one more additional term. In these cases the average CPU time was about 2 hours per

process, using the same machine. Since the rank of  $\mathfrak{D}$  is 3, the enumeration of the smallest ellipsoid took more time. The average CPU time of the enumeration of the smallest ellipsoids were 12 minutes.

In one of the processes the set  $\mathfrak{D}$  had rank 2, so we had to choose two additional terms in this case. The CPU time was about 124 hours. The enumeration of the smallest ellipsoid took 30 hours.

In the enumeration processes we have also used a simple modular sieve to test the vector found in the ellipsoids.

Finally we summarize the solutions of equation (6) we have found:

$$\begin{aligned} (x, y, z) \in \{ & (-1, 5, -5), (2, -3, -6), (0, 1, -1), (2, -2, -1), (3, -3, -2), \\ & (1, -1, -1), (1, -2, 1), (1, 1, 0), (1, -1, 0), (2, 1, -1), (0, 1, 1), \\ & (1, -2, -1), (2, -1, 0), (1, 0, -2), (0, 0, 1), (1, 0, 0), (1, 2, 1), \\ & (4, -4, 1), (-4, 9, 5), (-1, 2, 2), (0, 2, -1), (1, 0, -1), (0, 1, 0), \\ & (-2, 8, -7), (2, -3, 1), (1, -3, 1)\} \end{aligned}$$

The total CPU time was 175 hours on a PC with a Celeron 800 Mhz processor. We implemented the method in Maple and executed the programs in Windows.

## References

- [1] A.Baker and H.Davenport, *The equations  $3x^2 - 2 = y^2$  and  $8x^2 - 7 = z^2$* , Q. J. Math. Oxford, **20**, (1969), 129–137.
- [2] Y.Bilu and G.Hanrot, *Solving Thue equations of high degree*, J. Number Theory, **60** (1996), 373–392.
- [3] J.-H.Evertse and K.Györy, *Finiteness criteria for decomposable form equations*, Acta Arith. **50** (1988), 357–379.
- [4] U.Fincke and M.Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comput., **44** (1985), 463–471.
- [5] I.Gaál, *Diophantine equations and power integral bases*, Birkhäuser Boston, 2002.
- [6] I.Gaál and M.Pohst, *On the resolution of relative Thue equations*, Math. Comput., **71** (2002), 429–440.
- [7] K.Györy, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv., **54** (1979), 583–600.
- [8] K.Györy, *On the solutions of linear diophantine equations in algebraic integers of bounded norm*, Ann. Univ. Sci. Budapest Eötvös, Sect. Math., **22-23** (1979-1980), 225-233.

- [9] K.Györy, *Résultats effectifs sur la représentation des entiers par des formes décomposable*, Kingston, Canada, 1980.
- [10] K.Györy, *Some recent applications of  $S$ -unit equations*, *Astérisque*, **209** (1992), 17–38.
- [11] K.Györy, *Bounds for the solutions of decomposable form equations*, *Publ. Math. Debrecen*, **52** (1998), 1–31.
- [12] G.Hanrot, *Solving Thue equations without the full unit group*, *Math. Comp.*, **69** (2000), 395–405.
- [13] I.Járasi, *Computing small solutions of unit equations in three variables II: Resultant form equations*, in preparation
- [14] A.Pethő, *On the resolution of Thue inequalities*, *J. Symbolic Comp.*, **4** (1987), 103–109.
- [15] A.Pethő and R.Schulenberg, *Effektives Lösen von Thue Gleichungen*, *Publ. Math. Debrecen*, **34** (1987), 189–196.
- [16] N.Tzanakis and B.M.M. de Weger, *On the practical solution of the Thue equation*, *J. Number Theory*, **31** (1989), 99–132.
- [17] K.Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern*, *J. Number Theory*, **82** (2000), 188–224.