MATHEMATICS OF COMPUTATION
Volume 71, Number 237, Pages 429–440
S 0025-5718(01)01329-1
Article electronically published on June 29, 2001

ON THE RESOLUTION OF RELATIVE THUE EQUATIONS

ISTVÁN GAÁL AND MICHAEL POHST

ABSTRACT. An efficient algorithm is given for the resolution of relative Thue equations. The essential improvement is the application of an appropriate version of Wildanger's enumeration procedure based on the ellipsoid method of Fincke and Pohst.

Recently relative Thue equations have gained an important application, e.g., in computing power integral bases in algebraic number fields. The presented methods can surely be used to speed up those algorithms.

The method is illustrated by numerical examples.

INTRODUCTION

Let $M \subset K$ be algebraic number fields with $m = [M : \mathbb{Q}]$ and $n = [K : M] \geq 3$. The rings of integers of K, M will be denoted by $\mathbb{Z}_K, \mathbb{Z}_M$, respectively. Let $\alpha \in K$ be an integral generator of K over M, $\mu \in M$ an algebraic integer and η an arbitrary unit in M. In this paper we consider the **relative Thue equation**

$$N_{K/M}(X - \alpha Y) = \eta\mu \quad \text{in} \quad X, Y \in \mathbb{Z}_M. \tag{1}$$

According to the effective results by Baker [1], this equation has only finitely many solutions up to multiplication by units in M. We note that Baker's result was generalized and extended by several authors (for further literature and the latest effective bounds for the sizes of the solutions of (1), see Bugeaud and Győry [6]).

Following the standard arguments, $X - \alpha Y$ is usually written as the product of an element of K of given norm and powers of fundamental units of K. The bound obtained by Baker's method for the exponents in this representation is an exponential function of certain parameters of K involving a very large constant. Hence, although the effective bounds imply that the solutions of the equations can be found in a finite number of steps, these bounds do not at all allow us to enumerate all possible exponents below the bound and for a complete resolution of the equation.

The result of Baker and Davenport [2] initiated a constructive theory of diophantine equations by developing the first algorithms for reducing the effective bounds for the exponents in a numerical way, using diophantine approximation techniques. These methods were extended by Pethő and Schulenberg [15], de Weger [19], and now the reduction step seems to be solved satisfactorily.

Received by the editor April 3, 1998 and, in revised form, May 5, 1999.

2000 *Mathematics Subject Classification.* Primary 11Y50; Secondary 11D59.

Key words and phrases. Relative Thue equation, Baker's method, reduction, enumeration.

Research of the first author was supported in part by Grants 16791 and 16975 from the Hungarian National Foundation for Scientific Research.

Research of the second author was supported by the Deutsche Forschungsgemeinschaft.

The final step of solving the equations is the enumeration of the possible values of the exponents below the reduced bounds. For simple examples, this is a trivial problem, but it can become hopeless if the number of exponential variables is large, even if the reduced bound is small. For this reason, sieve methods are frequently applied in this step. Using sieve methods, Smart [18] developed an algorithm for solving relative Thue equations. For a detailed account of his parallel sieve, cf. Smart [17]. We expect our method to be much more efficient if the number of exponential variables is large. A comparison of our method with the sieve methods is given at the end of the paper.

Recently, Wildanger [21] introduced a new method for the enumeration of small values of the exponents, building ellipsoids by taking Euclidean norms of vectors in the logarithmic space, and applying the very efficient method of Fincke and Pohst [8] for enumerating lattice points in the ellipsoids. This method is suitable to solve the above-mentioned final enumeration problem efficiently.

Thue equations are one of the most important classes of diophantine equations, having also several applications. In the absolute case (for $M = \mathbb{Q}$) Bilu and Hanrot [4], [5] gave an efficient method avoiding the problem of final enumeration by eliminating the linear forms in several variables and considering only linear forms in two variables. Also, an idea of Pethő [14] makes it easy and fast to find small solutions of absolute Thue equations. However, even after a detailed investigation we did not see a possibility to adopt these methods to the relative case in order to make the algorithm more efficient.

It is important to remark that relative Thue equations recently gained an important application in computing power integral bases of algebraic number fields. In several cases (see, e.g., [9], [10], [11], [12], [13]), this problem was reduced to relative Thue equations.

These were actually the first results where *several* relative Thue equations were solved completely. We note that de Weger [20] solved a single relative Thue equation at about the same time. In all previous results, as well as in Smart [18], variants of sieve methods were used in the final enumeration step, consuming a considerable amount of CPU time.

In the present paper we show how an appropriate version of Wildanger's method can be used instead of sieving. We apply his ideas in a more complicated situation in which the unit equation involves power products of quotients of some relative conjugates of units with unknown exponents, instead of just power products of conjugates of units. In creating this version we have adjusted its formulation for the present type of problems, and we have also simplified its formulation as much as possible.

We briefly summarize how to use Baker's method and the reduction procedure to relative Thue equations and concentrate on the new ingredient of the algorithm in the last step.

Baker's method

Let $\eta_1, \dots, \eta_s$ be a system of fundamental units in M. Extend this system to a maximal independent system $\eta_1, \dots, \eta_s, \varepsilon_1, \dots, \varepsilon_r$ of units in K. Then any solution $X, Y \in \mathbb{Z}_M$ of (1) can be written as

$$X - \alpha Y = \nu(\eta_1)^{b_1} \dots (\eta_s)^{b_s} (\varepsilon_1)^{a_1} \dots (\varepsilon_r)^{a_r}. \tag{2}$$

Here $\nu \in \mathbb{Z}_K$ is an integral element with relative norm μ. Up to unit factors in K there are only finitely many possibilities for ν, which can be determined using the KANT package [7], and the following procedure must be performed for each possible value of ν.

The exponents $b_1, \dots, b_s, a_1, \dots, a_r$ in (2) are integers if the above system of independent units is a fundamental system of units. Otherwise, $b_1, \dots, b_s, a_1, \dots, a_r$ can have a common denominator. In order to make our presentation simpler, we assume that the exponents are integral; otherwise the formulae must be modified in a straightforward way.

Setting

$$X' = \frac{X}{(\eta_1)^{b_1} \dots (\eta_s)^{b_s}}, \quad Y' = \frac{Y}{(\eta_1)^{b_1} \dots (\eta_s)^{b_s}}$$

yields

$$X' - \alpha Y' = \nu(\varepsilon_1)^{a_1} \dots (\varepsilon_r)^{a_r}. \tag{3}$$

We will just calculate $a_1, \dots, a_r$, since the solutions of (1) are determined only up to unit factors of M.

For any $\gamma \in K$ we denote by $\gamma^{(11)}, \dots, \gamma^{(1n)}, \dots, \gamma^{(m1)}, \dots, \gamma^{(mn)}$ the conjugates of γ, so that for $1 \le i \le m$ the elements $\gamma^{(i1)}, \dots, \gamma^{(in)}$ are the corresponding relative conjugates of γ over the conjugate field $M^{(i)}$ of M. To simplify our notation, for any i $(1 \le i \le m)$ and any distinct j_1, j_2, j_3 $(1 \le j_1, j_2, j_3 \le n)$ we introduce a symbol $I = (ij_1j_2j_3)$ and set

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

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

and

$$\beta^{(I)} = \beta^{(ij_1j_2j_3)} = \frac{\left(\alpha^{(ij_2)} - \alpha^{(ij_3)}\right) \cdot (X' - \alpha Y')^{(ij_1)}}{\left(\alpha^{(ij_1)} - \alpha^{(ij_3)}\right) \cdot (X' - \alpha Y')^{(ij_2)}}.$$

Then we have

$$\beta^{(I)} = \gamma^{(I)}\tau^{(I)}.$$

Consider the system of linear equations

$$a_1 \log\left|\rho_1^{(I)}\right| + \dots + a_r \log\left|\rho_r^{(I)}\right| = \log\left|\tau^{(I)}\right| \tag{4}$$

in $a_1, \dots, a_r$ for any $I = (ij_1j_2j_3)$ with $1 \le i \le m$ and any distinct j_1, j_2, j_3 $(1 \le j_1, j_2, j_3 \le n)$ (the equations are independent of j_3). Since $\varepsilon_1, \dots, \varepsilon_r$ are independent over M, the matrix of coefficients on the left side has rank r. Choosing a set of r linearly independent equations and multiplying by the inverse of the coefficient matrix of the system, we conclude

$$A = \max(|a_1|, \dots, |a_r|) \le c_1 \cdot \left|\log\left|\tau^{(I)}\right|\right| \tag{5}$$

for a certain set $I = (ij_1j_2j_3)$ of indices, where c_1 is the row norm (maximum sum of the absolute values of the elements in a row) of the inverse matrix of the coefficient

matrix of (4). We choose a set of independent equations so that c_1 becomes as small as possible. Now if $|\tau^{(I)}| < 1$, then (5) implies

$$\left|\tau^{(I)}\right| < \exp\left(-\frac{A}{c_1}\right) \quad , \tag{6}$$

and if $|\tau^{(I)}| > 1$, then the same holds for $|\tau^{(I^*)}| = 1/|\tau^{(I)}| > 1$ with $I^* = (ij_2j_1j_3)$. From now on we assume that (6) is valid. The following procedure (application of Baker's method, reduction) must be performed for each possible value of i, j_1, j_2 since we cannot predict which of the $|\tau^{(I)}|$ satisfies the crucial inequality (6).

Let $1 \le j_3 \le n$ be any index distinct from j_1, j_2. Using Siegel's identity we have

$$\begin{aligned}(\alpha^{(ij_1)} - \alpha^{(ij_2)})(X' - \alpha^{(ij_3)}Y') + (\alpha^{(ij_2)} - \alpha^{(ij_3)})(X' - \alpha^{(ij_1)}Y') \\ + (\alpha^{(ij_3)} - \alpha^{(ij_1)})(X' - \alpha^{(ij_2)}Y') = 0.\end{aligned}$$

For $I = (ij_1j_2j_3)$ and $I' = (ij_3j_2j_1)$ we obtain

$$\beta^{(I)} + \beta^{(I')} = 1. \tag{7}$$

Using $|\log x| < 2|x-1|$ holding for all $|x-1| < 0.795$ and applying (6), from (7) we get

$$\left|\log\left(\beta^{(I')}\right)\right| \le 2 \cdot \left|\beta^{(I')} - 1\right| = 2 \cdot \left|\beta^{(I)}\right| \le c_2 \exp\left(-\frac{A}{c_1}\right) \quad , \tag{8}$$

where $c_2 = 2 \cdot |\gamma^{(I)}|$. On the other hand,

$$\begin{aligned}\left|\log\left(\beta^{(I')}\right)\right| = \Big|\log\left(\gamma^{(I')}\right) + a_1 \cdot \log\left(\rho_1^{(I')}\right) \\ + \ldots + a_r \cdot \log\left(\rho_r^{(I')}\right) + a_0 \cdot \log(-1)\Big| \quad ,\end{aligned} \tag{9}$$

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 $A \le A' \le rA + 1$. Note that (8) implies

$$\left|\log\left(\beta^{(I')}\right)\right| \le c_2 \exp\left(-\frac{A'-1}{rc_1}\right). \tag{10}$$

In the case that the terms in (9) are linearly independent, then we can directly apply the estimates of Baker and Wüstholz [3] to the linear form in (9) to derive a lower bound of type

$$\left|\log\left(\beta^{(I')}\right)\right| \ge \exp(-C \cdot \log A') \quad ,$$

which, compared to (10), implies an upper bound for A' and A.

Note that if $\log\left(\gamma^{(I')}\right)$ in (9) is dependent on the other terms, we can reduce the number of variables in the linear form. The variable a_0 can be omitted for totally real fields K.

The bounds obtained by Baker's method are about 10^{20} for $r = 2, 3$ and go up to about 10^{500} for $r = 7, 8$.

Reduction

Using (9) and (10) we have an estimate of type

$$|x_1\xi_1 + \ldots + x_k\xi_k| < c_2 \exp(-c_3 X - c_4) \ , \tag{11}$$

where $k = r+2, x_1 = 1, x_2 = a_1, \ldots, x_{r+1} = a_r, x_{r+2} = a_0$,

$$\begin{aligned}
\xi_1 &= \log\left(\gamma^{(I')}\right), \\
\xi_2 &= \log\left(\rho_1^{(I')}\right), \ldots, \xi_{r+1} = \log\left(\rho_r^{(I')}\right), \\
\xi_{r+2} &= \log(-1),
\end{aligned}$$

$X = \max(|x_1|, \ldots, |x_k|)$, and c_2, c_3, c_4 are positive constants. Let H be a large constant (to be specified later) and consider the lattice $\mathcal{L}$ spanned by the columns of the k by $k+2$ matrix

$$\begin{pmatrix}
1 & 0 & \ldots & 0 \\
0 & 1 & \ldots & 0 \\
\vdots & \vdots & \vdots & \vdots \\
0 & 0 & \ldots & 1 \\
H\Re(\xi_1) & H\Re(\xi_2) & \ldots & H\Re(\xi_k) \\
H\Im(\xi_1) & H\Im(\xi_2) & \ldots & H\Im(\xi_k)
\end{pmatrix}$$

Assume that the columns in the above matrix are linearly independent. Denote by b_1 the first vector of an LLL-reduced basis of this lattice.

Lemma 1. *If $X \le X_0$ and $|b_1| \ge \sqrt{(k+1)2^{k-1}} \cdot X_0$, then*

$$X \le \frac{\log H + \log c_2 - c_4 - \log X_0}{c_3}.$$

Proof. Denote by l_0 the shortest vector in the lattice and l_1 the shortest of those vectors having first coordinate 1. Using the inequalities of [16] we have $|b_1|^2 \le 2^{k-1}|l_0|^2$. Then by the assumptions, using also (11),

$$\begin{aligned}
2^{1-k}\left((k+1)\cdot 2^{k-1}X_0^2\right) &\le 2^{1-k}|b_1|^2 \\
&\le |l_0|^2 \le |l_1|^2 \le k\cdot X_0^2 + H^2 c_2^2 (\exp(-c_3X - c_4))^2 \ ,
\end{aligned}$$

whence

$$X_0 \le H c_2 \exp(-c_3 X - c_4) \ ,$$

which implies the assertion. □

If the terms in (11) are linearly dependent, then we can reduce the number of variables and we apply Lemma 1 with $k = r+1$. In this case x_1 is not restricted to 1, but for that case the assertion remains valid (just omit l_1 in the proof).

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 X_0 to be Baker's bound, apply Lemma 1 to reduce it to the constant in the assertion, and in the next step we use the new bound as X_0. An appropriate value of H corresponding to X_0 is of magnitude X_0^k. The reduction is very efficient: in the first steps the former bound is reduced almost to its logarithm. After about 4–5 steps, the procedure stabilizes; i.e., the new bound is not any smaller than the

previous bound. Then we stop the procedure. The final reduced bound is usually between 100 and 1000. Note that one can utilize $x_1 = 1$ to improve the reduction.

Final enumeration

Since we usually have $r \geq 3$ for relative Thue equations, it is a nontrivial problem to test all possible values of the exponents $a_1, \ldots, a_r$ below the reduced bounds. For larger values of r, this problem is actually the main difficulty in solving such equations. Our goal in this section is to show how an appropriate version of Wildanger's enumeration method [21] can be used for relative Thue equations.

Let $\mathcal{I} = \{I_1, \ldots, I_t\}$ be a set of tuples $I = (ij_1j_2j_3)$ with $1 \leq i \leq m$ and distinct $1 \leq j_1, j_2, j_3 \leq n$ with the following properties:

1. if $(ij_1j_2j_3) \in \mathcal{I}$, then either $(ij_2j_3j_1) \in \mathcal{I}$ or $(ij_3j_2j_1) \in \mathcal{I}$;
2. if $(ij_1j_2j_3) \in \mathcal{I}$, then either $(ij_1j_3j_2) \in \mathcal{I}$ or $(ij_3j_1j_2) \in \mathcal{I}$;
3. the vectors
$$\underline{e}_k = \begin{pmatrix} \log\left|\rho_k^{(I_1)}\right| \\ \vdots \\ \log\left|\rho_k^{(I_t)}\right| \end{pmatrix} \quad (1 \leq k \leq r)$$
are linearly independent.

Since $\varepsilon_1, \ldots, \varepsilon_r$ are multiplicatively independent over M, the last condition can be satisfied if we take sufficiently many tuples. Note that choosing a minimal set of tuples satisfying those conditions reduces the amount of necessary computations considerably.

Set
$$\underline{g} = \begin{pmatrix} \log\left|\gamma^{(I_1)}\right| \\ \vdots \\ \log\left|\gamma^{(I_t)}\right| \end{pmatrix}, \quad \underline{b} = \begin{pmatrix} \log\left|\beta^{(I_1)}\right| \\ \vdots \\ \log\left|\beta^{(I_t)}\right| \end{pmatrix}.$$

In our notation, we have

$$\underline{b} = \underline{g} + a_1\underline{e}_1 + \ldots + a_r\underline{e}_r \ . \tag{12}$$

We denote by A_0 the reduced bound for $A = \max(|a_1|, \ldots, |a_r|)$. Setting
$$\log S_0 = \max_{I \in \mathcal{I}} \left(\left|\log\left|\gamma^{(I)}\right|\right| + A_0 \left|\log\left|\rho_1^{(I)}\right|\right| + \ldots + A_0 \left|\log\left|\rho_r^{(I)}\right|\right| \right),$$
we obtain for any tuple I:

$$\frac{1}{S_0} \leq \left|\beta^{(I)}\right| \leq S_0. \tag{13}$$

The next lemma describes how we can replace S_0 by a smaller constant.

Lemma 2. *Let $1 < s < S$ be given constants and assume that*

$$\frac{1}{S} \leq \left|\beta^{(I)}\right| \leq S \quad \textit{for all} \quad I \in \mathcal{I}. \tag{14}$$

Then either

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

or there is an $I \in \mathcal{I}$ *with*

$$\left|\beta^{(I)} - 1\right| \leq \frac{1}{s-1}. \tag{16}$$

Proof. Assume that the tuple $I = (ij_1j_2j_3) \in \mathcal{I}$ violates (15). Set $I' = (ij_3j_2j_1)$ and $I'' = (ij_3j_1j_2)$. Then we have either

$$\frac{1}{S} \leq \left|\beta^{(I)}\right| \leq \frac{1}{s} \ ,$$

which together with (7) implies

$$\left|\beta^{(I')} - 1\right| \leq \frac{1}{s} \ , \tag{17}$$

or we have

$$s \leq \left|\beta^{(I)}\right| \leq S \ ,$$

yielding

$$\left|\beta^{(I'')} - 1\right| = \left|-\frac{\beta^{(I')}}{\beta^{(I)}} - 1\right| = \left|\frac{1}{\beta^{(I'')}}\right| \leq \frac{1}{s} \ . \tag{18}$$

If the tuple (I') is not in $\mathcal{I}$, but $I''' = (ij_2j_3j_1)$ is in $\mathcal{I}$, then $\beta^{(I''')} = 1/\beta^{(I')}$ and (17) imply

$$\left|\beta^{(I')} - 1\right| \leq \frac{1}{s-1} \ .$$

The case that I'' is not in $\mathcal{I}$, but $I'''' = (ij_1j_3j_2)$ is in $\mathcal{I}$ is treated analogously. □

Summarizing, the constant S can be replaced by the smaller constant s if for each j_0 $(1 \leq j_0 \leq t)$ we enumerate directly the set H_{j_0} of those exponents $a_1, \ldots, a_r$ for which

$$\begin{aligned} &\frac{1}{S} \leq \left|\beta^{(I)}\right| \leq S \quad \text{for all} \quad I \in \mathcal{I}, \\ &\left|\beta^{(I_{j_0})} - 1\right| \leq \frac{1}{s-1}. \end{aligned} \tag{19}$$

Next we consider the enumeration of the set H_{j_0}. We set

$$\lambda_j = \begin{cases} \frac{1}{\log S} & \text{for} \quad j \neq j_0,\ 1 \leq j \leq t \ , \\ \\ \frac{1}{\log \frac{s-1}{s-2}} & \text{for} \quad j = j_0 \ , \\ \\ \frac{1}{\arccos \frac{s(s-2)}{(s-1)^2}} & \text{for} \quad j = t+1 \ , \end{cases}$$

$$\varphi_{j_0}(\underline{b}) = \begin{pmatrix} \lambda_1 \log\left|\beta^{(I_1)}\right| \\ \vdots \\ \lambda_t \log\left|\beta^{(I_t)}\right| \\ \lambda_{t+1} \arg\left(\beta^{(I_{j_0})}\right) \end{pmatrix}, \qquad \varphi_{j_0}(\underline{g}) = \begin{pmatrix} \lambda_1 \log\left|\gamma^{(I_1)}\right| \\ \vdots \\ \lambda_t \log\left|\gamma^{(I_t)}\right| \\ \lambda_{t+1} \arg\left(\gamma^{(I_{j_0})}\right) \end{pmatrix},$$

and

$$\varphi_{j_0}(\underline{e}_k) = \begin{pmatrix} \lambda_1 \log \left|\rho_k^{(I_1)}\right| \\ \vdots \\ \lambda_t \log \left|\rho_k^{(I_t)}\right| \\ \lambda_{t+1} \arg\left(\rho_k^{(I_{j_0})}\right) \end{pmatrix} \qquad (1 \le k \le r) \quad ,$$

where $-\pi \le \arg z \le \pi$ for all $z \in \mathbb{C}$, and

$$\underline{e}_0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \pi \end{pmatrix} \in \mathbb{R}^{t+1} \quad .$$

Obviously, if $\underline{e}_1, \ldots, \underline{e}_r$ are multiplicatively independent, then their images $\varphi_{j_0}(\underline{e}_1), \ldots, \varphi_{j_0}(\underline{e}_r)$ are linearly independent and (12) implies that there exists an integer a_0 such that

$$\varphi_{j_0}(\underline{b}) = \varphi_{j_0}(\underline{g}) + a_1\varphi_{j_0}(\underline{e}_1) + \ldots + a_r\varphi_{j_0}(\underline{e}_r) + a_0\underline{e}_0 \quad . \tag{20}$$

Moreover, using (19), we obtain for the norm of this vector

$$\begin{aligned} &||\varphi_{j_0}(\underline{g}) + a_1\varphi_{j_0}(\underline{e}_1) + \ldots + a_r\varphi_{j_0}(\underline{e}_r) + a_0\underline{e}_0||_2^2 = ||\varphi_{j_0}(\underline{b})||_2^2 \\ &= \sum_{j=1}^{t} \lambda_j^2 \log^2 \left|\beta^{(I_j)}\right| + \lambda_{t+1}^2 \arg^2\left(\beta^{(I_{j_0})}\right) \le t+1 \end{aligned} \tag{21}$$

by the inequalities of [21, Lemma 1.13], which ensure that for the above choice of the parameters λ all summands are ≤ 1. Hence we have shown that inequality (21) holds for any $(a_1, \ldots, a_r) \in H_{j_0}$. This inequality defines an ellipsoid. The lattice points contained in this ellipsoid can be enumerated by using the algorithm of Fincke and Pohst [8]. The enumeration is usually very fast, but it is essential that the "improved" version of the algorithm should be used, involving LLL reduction.

Note that if $\underline{g}$ is dependent on $\underline{e}_1, \ldots, \underline{e}_r, \underline{e}_0$, then it is possible to reduce the number of variables. 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 (21) we only get t on the right-hand side.

Applying that procedure we obtain constants $S_0 > S_1 > \ldots > S_k$ by taking $S = S_i, s = S_{i+1}$ in each step, and we enumerate the lattice points in the corresponding ellipsoids. The initial constant is given by the reduced bound (see above), the last constant S_k should be made as small as possible, so that the exponents with

$$\frac{1}{S_k} \le \left|\beta^{(I)}\right| \le S_k \quad \text{for all} \quad I \in \mathcal{I} \tag{22}$$

can be enumerated easily. We observe that the set (22) is also contained in an ellipsoid; namely, by (12) we have

$$||\underline{g} + a_1\underline{e}_1 + \ldots + a_r\underline{e}_r||_2^2 = ||\underline{b}||_2^2 \le t \cdot (\log S_k)^2. \tag{23}$$

Usually, in the first enumeration step, S_1 can be much smaller than S_0, e.g., $S_1 = 10^{10}$ or 10^{20}. Then it is economical to take $S_{i+1} = \sqrt{S_i}$ until S_i decreases to about 10^3. Then we choose $S_{i+1} = S_i/2$. For an optimal choice of these constants we refer to Wildanger [21].

Numerical results

We illustrate our algorithm by two detailed examples. The first of them is a simple cubic equation over a quadratic field, which we solved earlier by using sieve methods. Hence, we wanted to compare the several hours of CPU time needed for sieving with the necessary CPU time needed for the enumeration with the ellipsoid method.

The second example is a more complicated one, which can hardly be solved by the sieve method.

For both examples we implemented our algorithm in MAPLE.

Example 1. Let $M = \mathbb{Q}(\sqrt{5})$ with basis element and fundamental unit $\eta = \omega = (1+\sqrt{5})/2$, and consider the equation

$$X^3 + (1-\omega)X^2Y + (-4+4\omega)XY^2 + (-8+5\omega)Y^3 = \pm\eta^k$$
$$\text{in} \quad X, Y \in \mathbb{Z}_M,\ k \in \mathbb{Z}\ .$$

The corresponding sextic field K has signature (4,2) with 4 fundamental units, η being among them. Hence in our linear forms, we had 3 unknown variables and the additional variable a_0 needed for the principal value of the logarithm. In the logarithmic linear forms, the term involving the α's is dependent on the other terms. Baker's method gave a bound 10^{37}. That was reduced in three steps to 1308, 199, 132, respectively. In the first reduction step, we took $H = 10^{155}$ and used a precision of 250 digits. The next steps were much easier, and the reduction procedure required only a few minutes.

In the final enumeration procedure, we had to consider 6 ellipsoids (i.e., we had to test 6 tuples $ij_1j_2j_3$). The vector $\underline{g}$ was dependent on the other vectors. The reduced bound 132 implied an initial constant $S_0 = 10^{497}$ to start the final enumeration. For this S_0 we made some trials to determine an optimal value of S_1, and our experience showed that even with $S_1 = 10^{10}$ the enumeration is very fast and gave no possible exponents. Then we took $S_2 = 10^4$; the second step was again very fast and gave no solutions. In the further steps, we had $S_3 = 1000, S_4 = 100, S_5 = 50$, and all possible exponents were enumerated very fast. It took only a few seconds to enumerate the ellipsoid (23). The solutions of the equation are

$$\begin{aligned}(X,Y) =&(1,0),(-1+\omega,1),(2-\omega,1),(-2+\omega,1),(0,-1-\omega),\\ &(12-7\omega,-5+3\omega),(-1+\omega,-4-8\omega),(4-3\omega,-2+2\omega)\end{aligned}$$

and of course all multiplies of them by units of M.

Example 2. Let $M = \mathbb{Q}(\sqrt{2})$ with basis element $\omega = \sqrt{2}$ and fundamental unit $\eta = 1+\sqrt{2}$. Consider the equation

$$X^4 - 2X^3Y + (-2-\omega)X^2Y^2 + (3+\omega)XY^3 + (1+\omega)Y^4 = \pm\eta^k$$
$$\text{in} \quad X, Y \in \mathbb{Z}_M,\ k \in \mathbb{Z}\ .$$

The corresponding octic field K is totally real with 7 fundamental units, among them η. Hence we had 6 unknown exponents. The term involving the α's was independent from the others in the logarithmic linear forms. Baker's method gave a bound 10^{53}, which was reduced in three steps to 1097, 121, 85, respectively. In the first reduction step we took $H = 10^{350}$ and used a precision of 420 digits. The next steps were much easier, and the whole reduction procedure required about five minutes.

In the final enumeration procedure we had to consider 18 ellipsoids (that is, we had to test 18 tuples $ij_1j_2j_3$). The vector $\underline{g}$ was independent from the other vectors. This means, that in fact we enumerated quadratic forms in 7 variables, one of them restricted to 1. The reduced bound 85 implied an initial constant $S_0 = 10^{269}$ for the final enumeration. We summarize the enumeration procedure in the following table. In the second and third columns $S > s$ denote the subsequent values $S_k > S_{k+1}$. In the fourth column Digits is the precision we used, the fifth column contains the number of tuples found (in the 18 ellipsoids together), and in the last column we display the running time (for the 18 ellipsoids together).

step	S	s	Digits	tuples	CPU time
1.	10^{269}	10^{50}	150	0	5 sec
2.	10^{50}	10^{20}	70	0	5 sec
3.	10^{20}	10^{12}	50	0	5 sec
4.	10^{12}	10^{10}	50	0	30 sec
5.	10^{10}	10^{8}	50	4	60 sec
6.	10^{8}	10^{7}	50	42	60 sec
7.	10^{7}	10^{6}	50	195	60 sec
8.	10^{6}	10^{5}	50	2081	180 sec
9.	10^{5}	$10^{4.5}$	50	2185	180 sec
10.	$10^{4.5}$	10^{4}	50	4957	180 sec
11.	10000	6000	50	5005	210 sec
12.	6000	3000	50	7274	240 sec
13.	3000	1500	50	8178	240 sec
14.	1500	1000	50	7306	180 sec
15.	1000	500	50	9113	240 sec
16.	500	250	50	10907	240 sec
17.	250	150	50	10077	240 sec
18.	150	100	50	9265	180 sec
19.	100	50	50	11431	180 sec
20.	50	40	50	6249	120 sec
21.	40	30	50	6297	120 sec
22.	30	20	50	6287	120 sec
23.	20	10	50	7039	120 sec
24.	10	5	50	4459	120 sec
25.	5	3	50	1306	70 sec
26.	3		50	5399	60 sec

The last line 26. corresponds to the single ellipsoid (23). The possible exponents were all tested if there were corresponding solutions (X, Y) of the equation; this took some seconds. The total CPU time for this example took about 1 hour. The solutions of the equation are

$$\begin{aligned}(X,Y) =&(-\omega, 1-\omega), (-1+\omega, -2+\omega), (\omega, -1), (-1, -1), (0, -1), (1, 0),\\ &(-1, -1+\omega), (2-\omega, -2+\omega), (-2, -1), (1, -\omega), (1-\omega, -1),\\ &(-4+\omega, -6+2\omega), (-1-\omega, \omega), (\omega, -2-2\omega), (-1, 2-\omega)\end{aligned}$$

and of course all multiples of them by units of M.

Comparison with the sieve method

Let us assume that we use the procedure with $S_0 > S_1 > \ldots > S_k$ and $\mathcal{I} = \{I_1, \ldots, I_t\}$. According to our notation

$$\log|\beta^{(I)}| = \log\left|\gamma^{(I)}\right| + a_1 \log\left|\rho_1^{(I)}\right| + \ldots + a_r \log\left|\rho_r^{(I)}\right|$$

satisfies the inequalities

$$\left|\log\left|\beta^{(I)}\right|\right| \le \begin{cases} \log S_{l-1} & \text{for} \quad I \in \mathcal{I} \setminus I_{j_0}, \\ \log \dfrac{S_l - 1}{S_l - 2} & \text{for} \quad I = I_{j_0}, \end{cases}$$

in the l-th step by (19). Then, following the arguments of Wildanger [21, p. 19] and taking into consideration also the final ellipsoid (23), we obtain that the number of steps needed for the enumeration is roughly proportional to

$$F = t \cdot \sum_{l=1}^{k} \left(\log \frac{S_l - 1}{S_l - 2}\right) (\log S_{l-1})^{t-1} + (\log S_k)^t .$$

At the beginning, the S_l are large but then $(S_l - 1)/(S_l - 2)$ is close to 1, so that its logarithm is close to 0. This makes the terms very small for large values of S_l. In the later steps the terms with small values of S_l are negligible. According to our computational experiences the number t of the ellipsoids to be enumerated is roughly $1.5\, r$ where r is the number of relative units.

As we have seen in Example 2, our method works within feasible running time even if the number of unknown exponents is 6. One could certainly improve the CPU time by a better choice of the constants S_1, S_2, etc. To make an optimal choice, cf. [21, pp. 19–21]. Note that Wildanger [21] applied this type of enumeration method even for unit rank 10 without difficulties.

When using the sieve method for r unknown exponents and taking a prime modulus p, the number of cases to test is $(p-1)^r$, which is already out of computational capacities for unit rank $r = 5$ if the prime is of magnitude 10^2. Note that the sieve method is only useful if the reduced bound A_0 for A is relatively large and we find an appropriate prime modulus p which is smaller than A_0. The prime p is to be chosen such that the minimal polynomial of the generating element of the field K splits into linear factors modulo p; hence usually $p > 100$.

References

1. A.Baker, *Transcendental number theory*, Cambridge University Press, 1975. MR **54:**10163
2. A.Baker & H.Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford **20** (1969), 129–137. MR **40:**1333
3. A.Baker & G.Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. **442** (1993), 19–62. MR **94i:**11050
4. Y.Bilu & G.Hanrot, *Solving Thue equations of high degree*, J. Number Theory **60** (1996), 373–392. MR **97k:**11040
5. Y.Bilu & G.Hanrot, *Thue equations with composite fields*, Acta Arith. **88** (1999), 311–326. MR **2000c:**11047
6. Y.Bugeaud & K.Győry, *Bounds for the solutions of Thue-Mahler equations and norm form equations*, Acta Arith. **74** (1996), 273–292. MR **97b:**11046
7. M. Daberkow, C.Fieker, J.Klüners, M.Pohst, K.Roegner & K.Wildanger, *KANT V4*, J. Symbolic Comp. **24** (1997), 267–283. MR **99g:**11150
8. U.Fincke & M.Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), 463–471. MR **86e:**11050

9. I.Gaál, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comp. **65** (1996), 801–822. MR **96g:**11155
10. I.Gaál, *Computing elements of given index in totally complex cyclic sextic number fields*, J. Symbolic Comp. **20** (1995), 61–69. MR **97a:**11173
11. I.Gaál, *Application of Thue equations to computing power integral bases in algebraic number fields*, Lecture Notes in Computer Science 1122, Proc. Conf. ANTS II, Talence, France, 1996, Springer, 1996, pp. 151–155. MR **97m:**11130
12. I.Gaál, *Solving index form equations in fields of degree nine with cubic subfields*, J. Symbolic Comp. **30** (2000), 181–193. CMP 2000:17
13. I.Gaál & M.Pohst, *On the resolution of index form equations in sextic fields with an imaginary quadratic subfield*, J. Symbolic Comp. **22** (1996), 425–434. MR **97m:**11161
14. A.Pethő, *On the resolution of Thue inequalities*, J. Symbolic Comp. **44** (1987), 103–109. MR **89b:**11030
15. A.Pethő & R.Schulenberg, *Effektives Lösen von Thue Gleichungen*, Publ. Math. (Debrecen) **34** (1987), 189-196. MR **89c:**11044
16. M.Pohst, *Computational Algebraic Number Theory*, DMV Seminar Band 21, Birkhäuser Verlag, Basel–Boston–Berlin, 1993. MR **94j:**11132
17. N.P.Smart, *The solution of triangularly connected decomposable form equations*, Math. Comp. **64** (1995), 819-840. MR **95f:**11110
18. N.P.Smart, *Thue and Thue-Mahler equations over rings of integers*, J. London Math. Soc. (2) **56** (1997), 455-462. MR **99d:**11031
19. B.M.M. de Weger, *Algorithms for diophantine equations*, CWI Tract 65., Amsterdam, 1989. MR **90m:**11205
20. B.M.M. de Weger, *A Thue equation with quadratic integers as variables*, Math. Comp. **64** (1995), 855–861. MR **95f:**11020
21. 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.

University of Debrecen, Mathematical Institute, H–4010 Debrecen Pf.12., Hungary
E-mail address: igaal@math.klte.hu

Technische Universität Berlin, Fakultät II, Institut für Mathematik, Strasse des 17. Juni 136, 10623 Germany
E-mail address: pohst@math.tu-berlin.de