Diophantine equations over global function fields I: The Thue equation

István Gaál a,1, Michael Pohst b,∗,2

a University of Debrecen, Mathematical Institute, H-4010 Debrecen Pf. 12, Hungary
b Technische Universität Berlin, Institut für Mathematik, Straße des 17. Juni 136, Berlin, Germany

Received 19 January 2004; revised 5 July 2005

Communicated by David Goss

Abstract

We solve completely Thue equations in function fields over arbitrary finite fields. In the function field case such equations were formerly only solved over algebraically closed fields (of characteristic zero and positive characteristic). Our method can be applied to similar types of Diophantine equations, as well.

© 2005 Published by Elsevier Inc.

MSC: 11D59; 11Y50; 11R58

Keywords: Thue equations; Global function fields

1. Introduction

Classical Diophantine equations like Thue equation (cf. Thue [10]) are traditionally solved over the rings of rational integers or over the ring of integers of a number field...
I. Gaál, M. Pohst / Journal of Number Theory

Several authors considered the analogous problem over function fields: more exactly over the ring of integers of a function field over an algebraically closed field, see, e.g., [6,8], both in case the ground field is of zero or positive characteristic. These results have also common generalizations (cf. Győry [5]).

Our purpose is now to investigate this problem in function fields over arbitrary finite fields. It is well known that Diophantine equations over finite fields play an important role in cryptography, cf. Niederreiter and Xing [7].

Also, from a practical point of view this case is much more straightforward than the case of algebraically closed ground fields (which mostly occur in theory only).

As it will turn out, also in this case the unit equation plays a crucial role and the solutions can be computed easily. However, for constructing the appropriate function fields, performing calculations in them, determining heights, etc. we intensively use the computer algebra package KASH [2].

2. Global function fields

In the following we shall strongly rely on the argument used by Mason [6] for function fields over algebraically closed fields. We show how his ideas can be transferred to our situation. A general description of properties of function fields (also over finite fields) can be found in the book of Stichtenoth [9].

We introduce some notations. \( k = \mathbb{F}_q \) denotes a finite field with \( q = p^d \) elements. The rational function field of \( k \) is \( k(t) \) as usual, and \( K \) is a finite extension of \( k(t) \) of degree \( n_0 \) and genus \( g_0 \). The integral closure of \( k[t] \) in \( K \) is denoted by \( o_K \). We assume that \( K \) is separably generated over \( k(t) \) by an element \( y \) belonging to \( o_K \) and that \( k \) is the full constant field of \( K \). Any element \( f \in K \) has a unique presentation

\[
f = \sum_{i=1}^{n_0} h_i y^{i-1}, \quad h_i \in k(t).
\]

Conjugates of elements (fields) are denoted by upper case indices. Let \( A := ((y^{(j)})^{i-1})_{1 \leq i, j \leq n} \in \mathbb{F}_q^{n \times n} \) have determinant \( D \). We note that \( D \) is the discriminant of \( y \). It is nonzero since \( K \) is separably generated. We obtain the system of linear equations:

\[
(f^{(1)}, \ldots, f^{(n)}) = (h_1, \ldots, h_n) A.
\]

Hence, the \( h_i \) are rational functions in the \( f^{(j)}, (y^{(j)})^{i-1} \).

The set of all (exponential) valuations of \( K \) is denoted by \( V \), the subset of infinite valuations by \( V_\infty \). By abuse of notation we do not distinguish between places and valuations. For example, we write \( \deg v \) for the degree of the divisor belonging to the valuation \( v \in V \).

For a nonzero element \( f \in K \) we denote by \( v(f) \) the value of \( f \) at \( v \). For integral elements this is the highest power of the divisor belonging to \( v \) that divides the divisor \( (f) \), and this
concept is extended to rational elements in the usual way. For the normalized valuations $v_N(f) = v(f) \cdot \deg v$ the product formula holds:

$$
\sum_{v \in V} v_N(f) = 0 \quad \forall f \in K \setminus \{0\}.
$$

The height of a nonzero element $f$ of $K$ is defined to be

$$
H(f) := \sum_{v \in V} \max\{0, v_N(f)\}.
$$

Because of the product formula this is tantamount to

$$
H(f) = -\sum_{v \in V} \min\{0, v_N(f)\}
$$

which then holds for all elements of $K$ including 0.

3. Unit equations

Let $V_0$ be a finite subset of $V$. Then the nonzero elements $\gamma \in K$ satisfying $v(\gamma) = 0$ for all $v \notin V_0$ form a multiplicative group in $K$. These elements are called $V_0$-units. For $V_0 = V_\infty$ the $V_0$-units are just the units of the ring $\mathcal{O}_K$.

The resolution of Thue equations (as well as several other types of classical Diophantine equations) is usually reduced to equations of the form

$$
\gamma_1 + \gamma_2 + \gamma_3 = 0 \quad (1)
$$

where the $\gamma_i$ are $V_0$-units for a suitable set $V_0$.

The crucial inequality of Mason on the above equation becomes in our case:

Lemma 3.1. Let $V_0$ be a finite subset of $V$ and let $\gamma_i$ ($1 \leq i \leq 3$) be $V_0$-units satisfying (1). Then either $\frac{\gamma_1}{\gamma_3}$ is in $K^p$ or its height is bounded:

$$
H\left(\frac{\gamma_1}{\gamma_3}\right) \leq 2g - 2 + \sum_{v \in V_0} \deg v. \quad (2)
$$

Proof. The proof is along the lines of the proof of Lemma 2 in [6] (see [6, p. 14]). Since in our case the field of constants $k$ is not algebraically closed we encounter a few additional difficulties which we will point out in what follows.
We may assume that \( f := \gamma_1/\gamma_3 \) and therefore \( \gamma_2/\gamma_3 = -f - 1 \) do not belong to \( k \). Let

\[
V_1 := \{ v \in V : v(f) < 0 \}, \quad V_2 := \{ v \in V : v(f) > 0 \}, \\
V_3 := \{ v \in V : v(f) = 0 \land v(f + 1) > 0 \}.
\]

These are disjoint subsets of the set \( V_0 \). Then we have

\[
H(f) = \sum_{v \in V_1} (-v(f)) \deg v = \sum_{v \in V_2} v(f) \deg v = \sum_{v \in V_3} v(f + 1) \deg v.
\]

This is true because of \( 1 = (1 + f) + (-f) \), the product formula, and the property \( v(f) < 0 \) \( \iff v(1 + f) < 0 \). If \( z \) denotes a prime element for the valuation \( v \in V \) then the differential \( 1 \cdot df \) satisfies \( v(1 \cdot df) = v(df/dz) \) (see [9, Chapter IV]). If \( f \) is not a \( p \)th power then the divisor \( 1 \cdot df \) is canonical, i.e., \( \deg(1 \cdot df) = 2g - 2 \), since the field \( k \) of constants is complete (see [9, Chapter I.5]). This yields

\[
2g - 2 = \sum_{v \in V} v(df) \deg v = \sum_{v \in V_0} v(df) \deg v = \sum_{v \in V_1 \cup V_2 \cup V_3} v(df) \deg v
\]

\[
\geq \sum_{v \in V_1 \cup V_2} (v(f) - 1) \deg v + \sum_{v \in V_3} (v(1 + f) - 1) \deg v
\]

\[
= -H(f) + H(f) - \sum_{v \in V_1 \cup V_2} \deg v + H(f) - \sum_{v \in V_3} \deg v
\]

\[
\geq H(f) - \sum_{v \in V_1 \cup V_2 \cup V_3} \deg v
\]

whence the assertion follows. \( \square \)

Taking \( \Phi = -\gamma_1/\gamma_3 \), \( \Psi = -\gamma_2/\gamma_3 \) Eq. (1) gives the unit equation in two variables

\[
\Phi + \Psi = 1 \tag{3}
\]

where \( \Phi, \Psi \) are \( V_0 \)-units. Because of characteristic \( p \) the number of solutions of such a unit equation can be infinite.

For example, if \( V_0 \) is just the set of infinite valuations and \( \eta, 1 - \eta \) are both units of \( \sigma K \) then also \( \eta^p, (1 - \eta)^p \) is a solution of (3) for every exponent \( \kappa = p^t \). Hence, there exist solutions of arbitrary large heights in this situation.

The subsequent lemma shows that for any finite subset \( V_0 \) of \( V \), the group of \( V_0 \)-units of \( K \) contains only a finite number, say \( s \), of \( V_0 \)-units \( \eta \) which are not \( p^t \)th powers and for which also \( 1 - \eta \) is a \( V_0 \)-unit. We denote the set of these units by \( \{ \eta_1, \ldots, \eta_s \} \).

**Lemma 3.2.** Let \( V_0 \) be a finite subset of \( V \). Assume that a \( V_0 \)-unit \( \Phi \) in \( K \) is a solution of (3). If \( \Phi \) is not a \( p^t \)th power of \( \eta_i \) (\( 1 \leq i \leq s \), \( \ell \in \mathbb{Z}_{\geq 0} \)) then \( \Phi \) belongs to a finite subset of \( K \) which can be calculated.
For the proof we refer to [6, Lemma 11, p. 98]. The proof starts by assuming that $\Phi$ is not a $p$th power in $K$ and therefore also provides the means to calculate the $\eta_i$.

4. Application to Thue equations

4.1. Preliminaries

We want to apply these results to (relative) Thue equations over $K$. Let

$$F(X, Y) := \sum_{i=0}^{n} A_i X^{n-i} Y^i \in \mathcal{O}_K[X, Y]$$

be a binary homogeneous form of degree at least 3. Without loss of generality (cf. [4, p. 20]) we can assume that $F$ is monic in $X$, i.e., $A_0 = 1$. The polynomial $F(X, 1) \in \mathcal{O}_K[X]$ is required to be separable and irreducible. Then for arbitrary $m \in \mathcal{O}_K$ the equation

$$F(x, y) = m \quad \text{in} \quad x, y \in \mathcal{O}_K$$

is called a Thue equation (over $K$). Denote by $\alpha$ a zero of $F(x, 1)$ in $\overline{K}$, let $L = K(\alpha)$ and $\mathcal{O}_L$ the integral closure of $k[t]$ in $L$. Assume that $k$ is the full constant field of $L$, too. If $x, y \in \mathcal{O}_K$ is a solution of the Thue equation then

$$F(x, y) = N_{L/K}(x - \alpha y) = m. \quad (4)$$

Denote by $\gamma(j) \ (j = 1, \ldots, n)$ the conjugates of any $\gamma \in L$ over $K$. Assume that $(x, y) \in \mathcal{O}_K^2$ is a solution of (4). Then $\beta = x - \alpha y$ is of norm $m$, that is $\beta$ can be represented in the form

$$\beta = x - \alpha y = \mu \cdot \eta \quad (5)$$

where $\eta$ is a unit in $L$ and $\mu$ is an element of a finite set $S$ of non-associated elements of $L$ of norm $m$ over $K$. For the solution of the corresponding norm equation we use the usual methods from algebraic number theory, i.e., calculate suitable $S$-units [3]. Those, together with Dirichlet’s unit theorem (cf., e.g., [11]), can be easily transferred to the function field case, too.

Denote by $\eta_1, \ldots, \eta_r$ a set of fundamental units in $L$ (that can be calculated by the computer algebra system KASH [2]). Setting $k^* = \langle \eta_0 \rangle$, there are integer exponents $a_0, a_1, \ldots, a_r$ such that

$$\beta = x - \alpha y = \mu \cdot \eta_0^{a_0} \cdot \eta_1^{a_1} \cdots \eta_r^{a_r}. \quad (6)$$
For fixed distinct $i, j, k$ (with $1 \leq i, j, k \leq n$) set $L_{ijk} = L(\alpha^{(i)}, \alpha^{(j)}, \alpha^{(k)})$ with genus $g$. Denote by $V_0$ a finite set of valuations of $L_{ijk}$ containing the infinite valuations and such that

$$v(\alpha^{(i)} - \alpha^{(j)}) = 0, \quad v(\alpha^{(j)} - \alpha^{(k)}) = 0, \quad v(\alpha^{(k)} - \alpha^{(i)}) = 0 \quad \text{if} \ v \notin V_0$$

and

$$v(\mu^{(i)}) = 0, \quad v(\mu^{(j)}) = 0, \quad v(\mu^{(k)}) = 0 \quad \text{if} \ v \notin V_0.$$ 

Siegel’s identity (holding trivially for any solution, see [4, Chapter 3]) gives

$$(\alpha^{(i)} - \alpha^{(j)})\beta^{(k)} + (\alpha^{(j)} - \alpha^{(k)})\beta^{(i)} + (\alpha^{(k)} - \alpha^{(i)})\beta^{(j)} = 0. \quad (7)$$

By the fundamental Lemma 3.1

$$\tau_{ijk} = \frac{(\alpha^{(i)} - \alpha^{(k)})\beta^{(i)}}{(\alpha^{(i)} - \alpha^{(j)})\beta^{(k)}}$$

is either of bounded height or is contained in $L_{ijk}$. In the following the height function is applied always in $L_{ijk}$.

4.2. Effective upper bounds for the solutions of Thue equations

In case Eq. (4) has only finitely many solutions we derive an upper bound for the heights of the solutions. If the equation has only finitely many solutions, then there must be $i, j, k$ such that $\tau_{ijk}$ is not a $p$th power in $L_{ijk}$. We keep the above notation and set $A = \max(H(\alpha^{(i)}), H(\alpha^{(j)}), H(\alpha^{(k)}))$.

**Theorem 4.1.** If $\tau_{ijk}$ is not a $p$th power, then Eq. (4) has only finitely many solutions and for all solutions $(x, y)$ we have

$$\max(H(x), H(y)) \leq 11A + \frac{1}{n}H(\mu) + 4g - 4 + 2 \sum_{v \in V_0} \deg v.$$ 

**Proof.** Applying Lemma 3.1 we get

$$H(\tau_{ijk}) \leq 2g - 2 + \sum_{v \in V_0} \deg v = c_1.$$ 

This implies

$$H\left(\frac{\beta^{(i)}}{\beta^{(k)}}\right) = H\left(\frac{x - \alpha^{(i)}y}{x - \alpha^{(k)}y}\right) \leq H(\tau_{ijk}) + H\left(\frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(j)} - \alpha^{(k)}}\right) \leq c_1 + 4A = c_2.$$
Using an argument of Mason [6, Chapter II.1] for \( y \neq 0 \) we have
\[
\frac{x}{y} = \frac{\alpha^{(k)} \beta^{(i)}/\beta^{(k)} - \alpha^{(i)}}{\beta^{(i)}/\beta^{(k)} - 1}
\]
whence
\[
H \left( \frac{x}{y} \right) \leq 2A + 2c_2.
\]
By
\[
y^n = \frac{\mu}{\prod_{h=1}^{n} \left( \frac{x}{y} - \alpha^{(h)} \right)}
\]
we derive
\[
nH(y) \leq H(\mu) + n \left( H \left( \frac{x}{y} \right) + A \right)
\]
whence the assertion follows for \( y \). The bound for \( x \) can be obtained similarly. \( \square \)

4.3. An algorithm for calculating the solutions of Thue equations

We now turn to finding the solutions of Eq. (4).

Case I. Consider first the case when \( \tau_{ijk} \) is of bounded height. Similarly as in the proof of Theorem 4.1 we obtain
\[
H \left( \frac{x - \alpha^{(i)} y}{x - \alpha^{(k)} y} \right) \leq H(\tau_{ijk}) + H \left( \frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(j)} - \alpha^{(k)}} \right) \leq c_1 + H \left( \frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(j)} - \alpha^{(k)}} \right) = c'_2. \quad (8)
\]
By (6) we have
\[
\frac{x - \alpha^{(i)} y}{x - \alpha^{(k)} y} = \frac{\mu^{(i)}}{\mu^{(k)}} \left( \frac{\eta^{(i)}_1}{\eta^{(k)}_1} \right)^{a_1} \cdots \left( \frac{\eta^{(i)}_r}{\eta^{(k)}_r} \right)^{a_r}
\]
whence using (8) we obtain
\[
H \left( \left( \frac{\eta^{(i)}_1}{\eta^{(k)}_1} \right)^{a_1} \cdots \left( \frac{\eta^{(i)}_r}{\eta^{(k)}_r} \right)^{a_r} \right) \leq c'_2 + H \left( \frac{\mu^{(k)}}{\mu^{(i)}} \right) = c_3.
\]
This means for any infinite valuation \( v \) of \( L_{ijk} \) we have
\[
a_1 \cdot v \left( \frac{\eta^{(i)}_1}{\eta^{(k)}_1} \right) + \cdots + a_r \cdot v \left( \frac{\eta^{(i)}_r}{\eta^{(k)}_r} \right) \leq c_3.
\]
Note that by interchanging $i$ and $k$ we get the same expression on the left-hand side with opposite sign: for this reason the inequalities are also valid with absolute values:

$$|a_1 \cdot v\left(\frac{\eta_1^{(i)}}{\eta_1^{(k)}}\right) + \cdots + a_r \cdot v\left(\frac{\eta_r^{(i)}}{\eta_r^{(k)}}\right)| \leq c_3.$$ (9)

Note that the units in the above formula have zero values at finite valuations. The inequalities of type (9) (obtained for different choices of $i, k$) can be used to determine all possible values of the exponents $a_1, \ldots, a_r$.

For any possible exponent vector $a_1, \ldots, a_r$ we can determine $\eta = \eta_1^{a_1} \cdots \eta_r^{a_r}$ in (5). Then the system of equations

$$x - \alpha^{(1)} y = \mu^{(1)} \cdot \eta^{(1)}, \quad x - \alpha^{(2)} y = \mu^{(2)} \cdot \eta^{(2)}$$

can be used to determine the corresponding $x, y$.

**Case II.** If in (7) we have

$$\tau_{ijk} = \frac{(\alpha^{(j)} - \alpha^{(k)})\beta^{(i)}}{(\alpha^{(i)} - \alpha^{(j)})\beta^{(k)}} \in L_{ijk}^p,$$

then using (5) we obtain

$$\frac{(\alpha^{(j)} - \alpha^{(k)})\mu^{(i)}}{(\alpha^{(i)} - \alpha^{(j)})\mu^{(k)}} \cdot \eta^{(i)} \in L_{ijk}^p.$$ Here the last term is a unit in $L_{ijk}$ hence for any finite valuation $v$ of $L_{ijk}$

$$v\left(\frac{(\alpha^{(j)} - \alpha^{(k)})\mu^{(i)}}{(\alpha^{(i)} - \alpha^{(j)})\mu^{(k)}}\right)$$

must be divisible by $p$. This usually does not hold and there is no Case II solution. Otherwise, $\tau_{ijk}$ is a $p$th power, say $\tau_{ijk} = \psi_{ijk}^p$, we replace $\tau_{ijk}$ by $\psi_{ijk}^p$ and repeat the argument.

**Remark.** In the above calculations several elements (e.g., $\alpha^{(i)} - \alpha^{(j)}$) are contained in subfields of type $L_{ij} = K(\alpha^{(i)}, \alpha^{(j)})$ of $L_{ijk}$. Since for elements in $L_{ij}$ the values at any valuation of $L_{ijk}$ can be easily calculated from the values of the corresponding valuations of $L_{ij}$, hence in fact almost all calculations can be performed in the subfields $L_{ij}$ which are much easier to deal with, especially for large degrees $n$.

5. Examples

**Example 1.** In the first example we do not need to apply the fundamental lemma.
Let \( k = \mathbb{F}_5 \), let \( K = k(t) \), let \( \alpha \) be a root of
\[
y^3 + t^7 + t = 0
\]
and let \( L = K(\alpha) \). Consider the Thue equation
\[
N_{L/k(t)}(x - \alpha y) = 1 \quad \text{in } x, y \in k[t]. \tag{10}
\]
Denote by \( \alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)} \) the conjugates of \( \alpha \). Using symmetric polynomials we have
\[
\alpha^{(3)} = -\alpha^{(1)} - \alpha^{(2)}
\]
and substituting it into \( \alpha^{(1)} \alpha^{(3)} + \alpha^{(2)} \alpha^{(3)} + \alpha^{(1)} \alpha^{(2)} = 0 \) we obtain
\[
(\alpha^{(2)})^2 + \alpha^{(1)} \alpha^{(2)} + (\alpha^{(1)})^2 = 0
\]
whence
\[
\alpha^{(2)} = \frac{4\alpha^{(1)} \pm \alpha^{(1)} \sqrt{-3}}{2} = 3(4\alpha^{(1)} \pm \alpha^{(1)} \sqrt{2}). \tag{11}
\]
Observe that \( \sqrt{2} \) is contained in \( \mathbb{F}_{25} \), a quadratic extension of \( K \), hence in this case
\[
M = L(\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}) = \mathbb{F}_{25}(t)(\alpha).
\]
Denote by \( w \) a generating element of the multiplicative group \( \mathbb{F}_{25}^\times \) of \( \mathbb{F}_{25} \) with
\[
2 = w^6, \quad 3 = w^{18}, \quad 4 = w^{12}.
\]
By (11) we have
\[
\alpha^{(2)} = w^{16} \alpha^{(1)}, \quad \alpha^{(3)} = w^8 \alpha^{(1)}.
\]
Siegel’s identity gets the form
\[
w^8(x - \alpha^{(1)} y) + (x - \alpha^{(2)} y) + w^{16}(x - \alpha^{(3)} y) = 0. \tag{12}
\]
In our case \( M \) has one infinite valuation. In the above equation all terms are units having zero values at all finite valuations. By the product formula their value at the infinite valuation is also 0, hence they are contained in the constant field \( \mathbb{F}_{25} \).

Equation (12) leads to the unit equation
\[
\frac{x - \alpha^{(1)} y}{x - \alpha^{(3)} y} + \frac{x - \alpha^{(2)} y}{x - \alpha^{(3)} y} = 1
\]
which can be written in the form

$$\varepsilon_1 + \varepsilon_2 = 1$$

in $\varepsilon_1, \varepsilon_2 \in \mathbb{F}_{25}^\times$. \hfill (13)

If $\varepsilon_1, \varepsilon_2$ are solutions of this equation, then

$$x - \alpha^{(1)} y = \varepsilon_1 w^4 (x - \alpha^{(3)} y), \quad x - \alpha^{(2)} y = \varepsilon_2 w^{20} (x - \alpha^{(3)} y),$$

hence (10) gets the form

$$\varepsilon_1 \varepsilon_2 (x - \alpha^{(3)} y)^3 = 1$$

whence for the solutions $\varepsilon_1, \varepsilon_2$ of (13) the $1/(\varepsilon_1 \varepsilon_2)$ must be a cube in $\mathbb{F}_{25}^\times$.

We determined all such solutions $\varepsilon_1, \varepsilon_2$ of (13), calculated the corresponding $x - \alpha^{(3)} y$ from (15) and determined $x, y$ from the system of linear equations (14). We found, that the only integer solution is $x = 1, y = 0$.

**Example 2.** Let $k = \mathbb{F}_{11}, K = k(t)$, let $\alpha$ be a root of

$$y^3 - ty + t^3 = 0$$

and let $L = K(\alpha)$. Consider the Thue equation

$$N_{L/k(t)}(x - \alpha y) = 1 \quad \text{in} \quad x, y \in k[t].$$

Denote by $\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}$ the conjugates of $\alpha$. Using symmetric polynomials we have

$$\alpha^{(3)} = -\alpha^{(1)} - \alpha^{(2)}$$

and substituting it into $\alpha^{(1)} \alpha^{(3)} + \alpha^{(2)} \alpha^{(3)} + \alpha^{(1)} \alpha^{(2)} = -t$ we obtain

$$(\alpha^{(2)})^2 + \alpha^{(1)} \alpha^{(2)} + (\alpha^{(1)})^2 - t = 0$$

whence

$$\alpha^{(2)} = \frac{-\alpha^{(1)} \pm \sqrt{-3(\alpha^{(1)})^2 + 4t}}{2}. \hfill (17)$$

The minimal polynomial of the square root is

$$z^6 + 5tz^4 + 9t^2z^2 + 5t^6 + 7t^3.$$

The function field $M = \mathbb{F}_{11}(t)(z)$ contains $\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}$. By

$$z^2 = -3(\alpha^{(1)})^2 + 4t$$
we have

$$\left(\alpha^{(1)}\right)^2 = \frac{-z^2 + 4t}{3}$$

whence

$$\alpha^{(1)} = \frac{6t^3 + 6t^2z^2 + tz^4}{t^4}.\]$$

Further we obtain

$$\alpha^{(2)} = \frac{-\alpha^{(1)} + z}{2}, \quad \alpha^{(3)} = \frac{-\alpha^{(1)} - z}{2}.\]$$

For any $1 \leq i \leq 3$ let $j = i + 1$ (mod 3), $k = i + 2$ (mod 3) (taking 3 in case of 0 remainder) and let

$$\gamma_i = (\alpha^{(j)} - \alpha^{(k)})(x - \alpha^{(i)}y).$$

Then Siegel’s identity gets the form

$$\gamma_1 + \gamma_2 + \gamma_3 = 0. \quad (18)$$

The field $M$ has genus 1. It has three infinite valuations, all of degree 2. The $x - \alpha^{(i)}y$ are units, having nonzero values only at the infinite valuations. The $(\alpha^{(i)} - \alpha^{(j)})/(\alpha^{(i)} - \alpha^{(j)})$ have nonzero values all together for 6 finite valuations, all having degrees 1 or 2, the sum of the degrees is 9. Denote by $V_0$ the set of these 6 finite and the three infinite valuations of $M$. Then by the fundamental Lemma 3.1 $\gamma_i/\gamma_j$ is either of bounded height, or is contained in $M^{11}$.

**Case I.** Assume

$$H\left(\frac{\gamma_1}{\gamma_3}\right) \leq 2 \cdot 1 - 2 + 15 = 15.$$

This implies

$$H\left(\frac{x - \alpha^{(1)}y}{x - \alpha^{(3)}y}\right) \leq 15 + H\left(\frac{\alpha^{(1)} - \alpha^{(2)}}{\alpha^{(2)} - \alpha^{(3)}}\right) = 17. \quad (19)$$

In our case $K$ has unit rank 1. The fundamental unit is

$$\varepsilon = 3t + 1 + 3\alpha.$$

The values

$$v\left(\frac{\varepsilon^{(i)}}{\varepsilon^{(k)}}\right)$$
(at infinite valuations) are $\pm 3$. Hence by (19) and (9) we have

$$x - \alpha y = \mu \cdot \varepsilon^a$$

with a root of unity $\mu$ in $k$, where

$$3 \cdot |a| \leq 17$$

hence

$$|a| \leq 5.$$ 

The possible values of $a$ were tested and we found only the solution $x = 1$, $y = 0$ for $a = 0$ and $x = 3r + 1$, $y = 8$ for $a = 1$.

**Case II.** To exclude $\gamma_1 \gamma_3 \in M^{11}$ we consider

$$\gamma_1 \gamma_3 = \frac{\alpha^{(2)} - \alpha^{(3)}}{\alpha^{(1)} - \alpha^{(2)}} \cdot \frac{x - \alpha^{(1)} y}{x - \alpha^{(3)} y}.$$ 

The second term on the right-hand side is a unit, hence

$$v \left( \frac{\alpha^{(2)} - \alpha^{(3)}}{\alpha^{(1)} - \alpha^{(2)}} \right)$$

should be divisible by 11 at all finite valuations $v$. This is not satisfied, however. (Similarly for $\gamma_1/\gamma_2$ and $\gamma_2/\gamma_3$.)

**Example 3.** Let $k = \mathbb{F}_3$, $K = k(t)$, let $\alpha$ be a root of

$$y^3 + (t^2 + 2)y^2 + (2t^2 + 2)y + 2 = 0$$

and let $L = K(\alpha)$. Consider the Thue equation

$$N_{L/k(t)}(x - \alpha y) = 1 \quad \text{in } x, y \in k[t].$$

(20)

Denote by $\alpha^{(1)}$, $\alpha^{(2)}$, $\alpha^{(3)}$ the conjugates of $\alpha$. Using symmetric polynomials we have

$$\alpha^{(3)} = -t^2 - 2 - \alpha^{(1)} - \alpha^{(2)}$$

and substituting it into $\alpha^{(1)}\alpha^{(3)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(1)}\alpha^{(2)} = 2t^2 + 2$ we obtain

$$(\alpha^{(2)})^2 + \alpha^{(2)}(\alpha^{(1)} + t^2 + 2) + (\alpha^{(1)})^2 + \alpha^{(1)}(t^2 + 2) + 2t^2 + 2 = 0$$
whence

\[ \alpha^{(2)} = -\frac{\alpha^{(1)} + t^2 + 2}{2} \pm \frac{\sqrt{\alpha^{(1)}(t^2 + 2) + t^4 + 2t^2 + 2}}{2}. \] (21)

The minimal polynomial of the square root is

\[ z^6 + z^4(t^4 + t^2 + 1) + z^2(t^8 + 2t^6 + 2t^2 + 1) + 2t^8 + 2t^4 + t^6 + 2. \]

The function field \( M = \mathbb{F}_3(t)(z) \) contains \( \alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)} \). By

\[ z^2 = \alpha^{(1)}(t^2 + 2) + t^4 + 2t^2 + 2, \]

we have

\[ \alpha^{(1)} = \frac{z^2 - t^4 - 2t^2 - 2}{t^2 + 2}. \]

Further we obtain

\[ \alpha^{(2)} = \frac{-\alpha^{(1)} - t^2 - 2 + z}{2}, \quad \alpha^{(3)} = \frac{-\alpha^{(1)} - t^2 - 2 - z}{2}. \]

For any \( 1 \leq i \leq 3 \) let \( j = i + 1 \mod 3 \), \( k = i + 2 \mod 3 \) (taking 3 in case of 0 remainder) and let

\[ \gamma_i = (\alpha^{(j)} - \alpha^{(k)})(x - \alpha^{(i)}y). \]

Then Siegel’s identity gets the form

\[ \gamma_1 + \gamma_2 + \gamma_3 = 0. \] (22)

The field \( M \) has genus 7. It has six infinite valuations, all of degree 1. The \( x - \alpha^{(i)}y \) are units, having nonzero values only at the infinite valuations. The \( (\alpha^{(i)} - \alpha^{(j)})/(\alpha^{(i)} - \alpha^{(j)}) \) have nonzero values all together for six finite valuations, all having degrees 4. Denote by \( V_0 \) the set of these six finite and the six infinite valuations of \( M \). Then by the fundamental Lemma 3.1 \( \gamma_i/\gamma_j \) is either of bounded height, or is contained in \( M^3 \).

**Case I.** Assume

\[ H\left( \frac{\gamma_1}{\gamma_3} \right) \leq 2 \cdot 7 - 2 + 24 = 42. \]

This implies

\[ H\left( \frac{x - \alpha^{(1)}y}{x - \alpha^{(3)}y} \right) \leq 42 + H\left( \frac{\alpha^{(1)} - \alpha^{(2)}}{\alpha^{(2)} - \alpha^{(3)}} \right) = 48. \] (23)
In this case $K$ has unit rank 2. The fundamental units are
\[ \varepsilon_1 = 1 + 2t^2\alpha + 2\alpha^2, \quad \varepsilon_2 = t^2 + 1 + (2t^2 + 1)\alpha + 2\alpha^2. \]

Considering the values of
\[ v\left( \frac{\varepsilon^{(i)}}{\varepsilon^{(k)}} \right) \]
(at infinite valuations) by (23) and (9) become
\[ x - \alpha y = \mu \cdot \varepsilon_1^{a_1} \cdot \varepsilon_2^{a_2} \]
with a root of unity $\mu$ in $k$, where
\[ |a_1 + 2a_2| \leq 24, \quad |a_1 - a_2| \leq 24, \]
whence
\[ |3a_1| \leq |a_1 + 2a_2| + |a_1 - a_2| \leq 48, \]
that is $|a_1| \leq 16$. Searching over the set
\[ -16 \leq a_1 \leq 16, \quad a_1 - 24 \leq a_2 \leq a_1 + 24 \]
we found the following solutions
\[ (x, y) = (1, 2t^2 + 1), (0, 2), (1, 1), (1, 0), (2t^2 + 2, 2t^2 + 1), (t^4 + 2t^2 + 1, 2t^2 + 1). \]

**Case II.** To exclude $\gamma_1, \gamma_3 \in M^3$ we consider
\[ \frac{\gamma_1}{\gamma_3} = \frac{\alpha^{(2)} - \alpha^{(3)}}{\alpha^{(1)} - \alpha^{(2)}} \cdot \frac{x - \alpha^{(1)} y}{x - \alpha^{(3)} y}. \]
The second term on the right-hand side is a unit, hence
\[ v\left( \frac{\alpha^{(2)} - \alpha^{(3)}}{\alpha^{(1)} - \alpha^{(2)}} \right) \]
should be divisible by 3 at all finite valuations $v$. This is not satisfied, however. (Similarly for $\gamma_1/\gamma_2$ and $\gamma_2/\gamma_3$.)

**Example 4.** Let $k = \mathbb{F}_5$, $K = k(t)$. For simplicity take $A = t^2 + t + 1$; $B = t^4 - 1$. Let $\alpha$ be a root of
\[ y^4 - 2B^2y^2 + A + B^2 = 0, \]
that is $\alpha = \sqrt{B + \sqrt{-A}}$, and let $L = K(\alpha)$. This function field $L$ obviously has $N = K(\sqrt{-A})$ as a subfield. Consider the Thue equation

$$N_{L/k}(x - \alpha y) = 1 \quad \text{in } x, y \in k[r]. \quad (24)$$

Denote by $\alpha^{(i)}$ the conjugates of $\alpha$ $(i = 1, \ldots, 4)$.

If we let

$$\alpha^{(1)} = \sqrt{B + \sqrt{-A}}, \quad \alpha^{(2)} = -\sqrt{B + \sqrt{-A}}$$

then by $\alpha^{(1)}\alpha^{(2)} = \sqrt{A + B^2}$. The element $\beta = \alpha^{(1)} + \alpha^{(1)}\alpha^{(2)}$ generates a function field $M$ of degree 8 over $K$ containing all conjugates of $\alpha$. The element $\beta$ is defined by the polynomial

$$z^8 + (-4B - 4A - 4B^2)z^6 + (4BA + 4B^3 + 6B^2 + 2A + 6A^2 + 6B^4 + 12AB^2)z^4$$

$$+ (-4BA + 12A^2 - 12B^4A + 16AB^2 + 4BA^2 + 4B^5 + 4B^{-4} - 12A^2B^2 - 4A^3$$

$$- 4B^3 + 8B^3A - 4B^6)z^2$$

$$+ (6B^4A^2 - B^4 - 4B^5 + 6B^6 + 2A^2 + 2AB^2 + 4BA^2 - 4B^7 - 8B^3A$$

$$+ 14B^4A + A^4 + 4A^3B^2 + 10A^2B^2 - 4BA^2 - 12B^5A - 4BA^3 - 12A^2B^3 + B^8)$$

$$= z^8 + (t^8 + 4t^4 + t^2 + t + 1)z^6 + (t^{16} + 2t^{10} + 2t^9 + 2t^8 + 2t^4 + 2t^3 + 3t^2$$

$$+ 2t + 4)z^4 + (t^{24} + 3t^{20} + 3t^{18} + 3t^{17} + 2t^{16} + t^{14} + t^{13} + 4t^{12} + t^{11} + 4t^{10}$$

$$+ t^9 + 2t^8 + t^7 + t^6 + 2t^4 + 4t^3 + 4t^2 + 2)z^2$$

$$+ (t^{32} + 3t^{28} + 4t^{26} + 4t^{25} + t^{24} + 4t^{22} + 4t^{21} + 2t^{19} + 2t^{18} + t^{17} + 3t^{15}$$

$$+ 2t^{14} + t^{13} + t^{12} + 2t^{11} + 3t^{10} + 4t^8 + 2t^7 + 3t^6 + 4t^5 + 2t^4 + 2t^3 + 4t^2).$$

By

$$\beta - \alpha = \sqrt{A + B^2} \quad (25)$$

we get

$$\beta^2 - 2\beta\alpha + \alpha^2 - A - B^2.$$ 

One of the roots of this equation satisfies the quartic defining polynomial of $\alpha$, giving the embedding of $\alpha^{(1)}$ into $M$. The other conjugate can be obtained by (25), the last two conjugates are the negatives of these ones.

The field $K$ has unit rank 3, we embed all conjugates of the fundamental units into $M$. (These units are far too complicated to include explicitly here.) Let
\[ \gamma_1 = (\alpha(2) - \alpha(3))(x - \alpha(1)y), \]
\[ \gamma_2 = (\alpha(3) - \alpha(1))(x - \alpha(2)y), \]
\[ \gamma_3 = (\alpha(1) - \alpha(2))(x - \alpha(3)y), \]
then we have
\[ \gamma_1 + \gamma_2 + \gamma_3 = 0. \] (26)

The field \( M \) has genus 13. It has eight infinite valuations, all of degrees 1. The \( x - \alpha(i)y \) are units, having nonzero values only at the infinite valuations. The quotients
\[ \frac{\alpha(1) - \alpha(2)}{\alpha(1) - \alpha(3)}, \quad \frac{\alpha(2) - \alpha(3)}{\alpha(2) - \alpha(1)}, \quad \frac{\alpha(3) - \alpha(1)}{\alpha(3) - \alpha(2)} \]
have nonzero values all together at four finite valuations, two of them being of degree 4, the other two of degree 6. Denote by \( V_0 \) the set of the eight infinite and these four finite valuations. Then by the fundamental Lemma 3.1 \( \gamma_i/\gamma_j \) is either of bounded height, or is contained in \( M^5 \).

**Case I.** Assume
\[ H\left( \frac{\gamma_1}{\gamma_3} \right) \leq 2 \cdot 13 - 2 + (8 + 12 + 8) = 52. \]
This implies
\[ H\left( \frac{x - \alpha(1)y}{x - \alpha(3)y} \right) \leq 52 + H\left( \frac{\alpha(1) - \alpha(2)}{\alpha(2) - \alpha(3)} \right) = 65. \] (27)
As we mentioned above, \( K \) has unit rank 3. We denote by \( \varepsilon_1, \varepsilon_2, \varepsilon_3 \) the fundamental units. Considering the values of
\[ v\left( \frac{\varepsilon^{(i)}_h}{\varepsilon^{(k)}_h} \right) \]
(at infinite valuations) for \( h = 1, 2, 3 \), by (27) and (9) we become
\[ x - \alpha y = \mu \cdot \varepsilon^{a_1}_1 \cdot \varepsilon^{a_2}_2 \cdot \varepsilon^{a_3}_3 \]
with a root of unity \( \mu \) in \( k \) where among others the exponents satisfy
\[ |50a_1 + 6a_2 + 54a_3| \leq 65, \]
\[ |51a_1 + 5a_2 + 54a_3| \leq 65, \]
\[ |49a_1 + 3a_2 + 54a_3| \leq 65. \]
There are about 8000 solutions \((a_1, a_2, a_3)\) of the above system of linear inequalities. Testing all possible exponent vectors we found that Eq. (24) has only the trivial solutions \((x, y) = (1, 0), (2, 0), (3, 0), (4, 0)\) (these yield in fact the multiples of \(x - \alpha y\) for \(x = 1, y = 0\) with roots of unity in \(k\)).

**Case II.** To exclude \(\frac{\gamma_1}{\gamma_3} \in M^5\) we consider

\[
\frac{\gamma_1}{\gamma_3} = \frac{\alpha^{(2)} - \alpha^{(3)}}{\alpha^{(1)} - \alpha^{(2)}} \cdot \frac{x - \alpha^{(1)} y}{x - \alpha^{(3)} y}.
\]

The second term on the right-hand side is a unit, hence

\[
v\left(\frac{\alpha^{(2)} - \alpha^{(3)}}{\alpha^{(1)} - \alpha^{(2)}}\right)
\]

should be divisible by 5 at all finite valuations \(v\). This is not satisfied, however. (Similarly for \(\gamma_1/\gamma_2\) and \(\gamma_2/\gamma_3\).)

**Computational experiences.** All computations used in the examples were performed by using the computer algebra system KASH [2], running on 1 GHz PC-s. The calculations took just some seconds with the exception of the test of about 8000 possible exponent vectors in Example 4 which took about 90 minutes.

**Acknowledgment**

The authors are thankful to the referee for his/her valuable remarks that lead to an improvement of the paper.

**References**