Diophantine equations over global function fields IV: S-unit equations in several variables with an application to norm form equations

István Gaál *
University of Debrecen, Mathematical Institute
H–4010 Debrecen Pf.12., Hungary
e–mail: igaal@math.klte.hu

and Michael Pohst †
Technische Universität Berlin, Institut für Mathematik
Straße des 17. Juni 136, Berlin, Germany
e-mail: pohst@math.tu-berlin.de

June 22, 2008

Abstract

We describe an efficient algorithm to calculate all solutions of unit equations in several variables over global function fields. Note that using the present tools it is not possible to solve completely unit equations in more than two variables over number fields. In the function field case such equations are completely solved here for the first time. As a typical application we determine all solutions of norm form equations.

*Research supported in part by K67580 and T048791 from the Hungarian National Foundation for Scientific Research

†Research supported by the Deutsche Forschungsgemeinschaft

2000 Mathematics Subject Classification: 11Y50; 11D57
Keywords: global function fields; unit equations; norm form equations

1 Introduction

Unit equations of type

$$u_1 + \ldots + u_n = 1$$

where u_i are elements in a unit group of a number field or a function field, play an essential role in the theory and in applications of diophantine equations. For example, Thue equations and index form equations can be reduced to unit equations in two variables. General norm form equations lead to unit equations in several variables. J.H.Evertse and K.Győry [2] showed that any decomposable form equation is equivalent to a system of unit equations in several variables.

In the *number field case* Baker's theory and reduction procedures allow to solve unit equations in two variables, cf. I.Gaál [3]. However, using the presently known tools it is hardly possible to solve unit equations in three or more variables. So, I.Járási [8] was only able to calculate "small" solutions of unit equations in three variables.

In the *function field case* unit equations in two variables were considered by R.C.Mason [9] and unit equations in several variables by R.C.Mason [10], [11]. In these cases it was assumed that the constant field is algebraically closed, both for characteristic zero and finite characteristic.

In [4], [5] and [6] we considered *function fields over finite fields.* We developed an algorithm for solving unit equations in two variables and also Thue equations over such function fields. In the present paper we give an effective algorithm for solving unit equations in three variables: this is the first time that such unit equations are completely solved. This algorithm has several applications. Here, we describe an efficient method for solving certain norm form equations.

2 Auxiliary results

Let $k = \mathbb{F}_q$ denote 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 and genus g. 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 z belonging to O_K and that k is the full constant field of K. The set of all (exponential) *valuations* of K is denoted by V, the subset of infinite valuations by V_∞. For a non-zero element $f \in K$ we denote by $v(f)$ the valuation of f at v. For the *normalized valuations* $v_N(f) = v(f) \cdot \deg v$ the *product formula*

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

holds. The *height* of a non-zero element f of K is defined to be

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

The following statements are generalizations of certain arguments of R.C.Mason [11].

For any $f \in K$ but not in K^p the *genus* g of the function field K is given by

$$2g - 2 = \sum_{v \in V} v\left(\frac{df}{dv}\right) \deg v. \tag{1}$$

For any $f \in K$ and any valuation $v \in V$ we have

$$v\left(\frac{df}{dv}\right) = v(f) - 1 \quad \text{if} \quad p \not| v(f), \quad v\left(\frac{df}{dv}\right) \geq v(f) \quad \text{if} \quad p | v(f). \tag{2}$$

Using the product formula, equations (1) and (2) yield for any $f \in K \setminus K^p$

$$\sum_{p | v(f)} \left(v\left(\frac{df}{dv}\right) - v(f) \right) \deg v = 2g \,-\, 2 \,+\, \sum_{p \not| v(f)} \deg v \;\; . \tag{3}$$

3 Unit equations in two variables

Let V_0 be a finite subset of V, containing the infinite valuations. Then the non-zero 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 O_K.) We consider the unit equation

$$\gamma_1 + \gamma_2 + \gamma_3 = 0 \tag{4}$$

where the γ_i are V_0-units for a suitable set V_0.

Note that equation (4) can be written in the form

$$\left(-\frac{\gamma_1}{\gamma_3}\right) + \left(-\frac{\gamma_2}{\gamma_3}\right) = 1$$

which is a unit equation in two variables.

Remark It suffices to assume that the $\gamma_1/\gamma_3, \gamma_2/\gamma_3$ are V_0-units which makes the set V_0 smaller, cf. the proof of Lemma 3.1 in [4].

When considering the general case we shall proceed by induction reducing the number of variables. The final step is the case $n = 3$ which we excerpt from [4] for the convenience of the reader.

Lemma 3.1 *Let V_0 be a finite subset of V and let γ_i $(1 \le i \le 3)$ be V_0-units satisfying (4). Then either $\frac{\gamma_1}{\gamma_3}$ is in K^p or its height is bounded:*

$$H\left(\frac{\gamma_1}{\gamma_3}\right) \le 2g - 2 + \sum_{v \in V_0} \deg v \ . \tag{5}$$

4 The general case: Reduction of the number of variables

Let V_0 be a finite subset of V containing the infinite valuations. Let γ_i, $(i = 1, \ldots, n)$ be V_0-units. The equation

$$\gamma_1 + \ldots + \gamma_n = 0 \tag{6}$$

is equivalent with the unit equation

$$\left(-\frac{\gamma_1}{\gamma_n}\right) + \ldots \left(-\frac{\gamma_{n-1}}{\gamma_n}\right) = 1 \tag{7}$$

in $n-1$ variables. (Note that the remark at the end of the previous section holds here, as well: it suffices if the above fractions are V_0-units.) The reason to consider unit equations in more than two variables is that several well known diophantine equations (e.g. norm form equations, resultant form equations) lead to such unit equations.

In this section we show how to describe all solutions of equation (7) by the solutions of a unit equation in a smaller number of variables.

Theorem 4.1 *Let V_0 be a finite subset of V and let γ_i $(1 \leq i \leq n)$ be V_0-units satisfying (6). Assume that no proper subsum of the sum in (6) vanishes. Then we can explicitly construct a finite subset N of V, a solution x_{1n} of the $V_0 \cup N$-unit equation*

$$x_{1n} + x_{3n} + \ldots x_{n-1,n} \;=\; 1 \;\;,$$

and a $V_0 \cup N$-unit Φ satisfying

$$H(\Phi) \leq 2g \,-\, 2 \,+\, \sum_{v \in V_0} \deg v \;\;, \tag{8}$$

such that

$$\frac{\gamma_1}{\gamma_n} \;=\; x_{1n} \cdot \Phi \;. \tag{9}$$

Proof of Theorem 4.1. We divide all terms in equation (6) by γ_2 and apply local derivation at an arbitrary valuation v to obtain

$$x_1 + x_3 + \ldots x_n \;=\; 0 \tag{10}$$

for $x_i := (\gamma_i/\gamma_2)'$ $(i = 1, 3, \ldots, n)$. (For simplicity, we denote by $(.)'$ the local derivative at v.) The last equation is a unit equation of type (6), but with a smaller number of variables. However, besides the valuations in V_0 additional valuations may appear for which the value of one of the x_i is non–zero. The set of such "new" valuations is denoted by N. The valuations $v \in N$ satisfy

$v(\gamma_i) = 0 \quad (1 \leq i \leq n)$, therefore also $v(\gamma_i/\gamma_2) = 0 \quad (i = 1, 3, \ldots, n)$, but $v(x_i) = v((\gamma_i/\gamma_2)') \neq 0$ for at least one $i \in \{1, 3, \ldots, n\}$. We set $J := \{i \in \{1, 3, \ldots, n\} \mid \exists v \in V \setminus V_0 \ v(x_i) \neq 0\}$. (We note that $v(x_i) > 0$ in this case because of (2).) Then we put

$$f \ := \ \prod_{j \in J} \frac{\gamma_j}{\gamma_2} \ .$$

For $v \in N \cup V_0$ we then have $v(f) = 0$, hence $p | v(f)$, and $v(f') > 0$ for $v \in N$. We also know that $v(f') - v(f) \geq 0$ for all v with $p | v(f)$. Using these inequalities and (3) we obtain

$$\begin{aligned} \sum_{v \in N} \deg v \quad & \leq \quad \sum_{v \in N} v(f') \ \deg v = \sum_{v \in N} (v(f') - v(f)) \ \deg v \\ & \leq \quad \sum_{p | v(f)} (v(f') - v(f)) \ \deg v = 2g - 2 + \sum_{p \not| v(f)} \deg v \\ & \leq \quad 2g - 2 + \sum_{v \in V_0} \deg v. \end{aligned} \tag{11}$$

Here, the last equation is correct only if f is not a p-th power. But that is guaranteed because of $v(f') > 0$.

Note that the valuations in N can be explicitly constructed. For this purpose recall that $t^{q^m} - t$ is the product of all monic irreducible polynomials of $k[t]$ whose degree divides m. The finite valuations of degree $\leq m$ of O_K can all be obtained by splitting in O_K the valuations of $k[t]$ belonging to monic irreducible polynomials with degrees $\leq m$.

By (10) we obtain that $x_{in} = -x_i/x_n \ \ (i = 1, 3, \ldots, n-1)$ are solutions of the $V_0 \cup N$–unit equation

$$x_{1n} + x_{3n} + \ldots + x_{n-1,n} \ = \ 1 \tag{12}$$

in a smaller number of variables.

Let Φ be the element satisfying

$$\frac{\gamma_1}{\gamma_n} = -\frac{x_1}{x_n} \cdot \Phi \tag{13}$$

that is

$$-\Phi = \frac{\gamma_1}{\gamma_n} \cdot \frac{x_n}{x_1} = \frac{\frac{\gamma_1}{\gamma_2}}{\frac{\gamma_n}{\gamma_2}} \cdot \frac{\left(\frac{\gamma_n}{\gamma_2}\right)'}{\left(\frac{\gamma_1}{\gamma_2}\right)'} =: \frac{\frac{1}{f} \cdot f'}{\frac{1}{h} \cdot h'} \quad , \tag{14}$$

where $f = \gamma_n/\gamma_2$, $h = \gamma_1/\gamma_2$, and f', h' denote the corresponding local derivatives at an arbitrary valuation v.

Using (2), considering separately the four cases according to whether $v(f)$ and $v(h)$ are divisible by p or not, and applying (3), we obtain

$$\begin{aligned}
H(\Phi) &= -\sum_{v \in V} \min(0, v(\Phi)) \, \deg v \\
&= -\sum_{v \in V} \min(0, v(f') - v(f) + v(h) - v(h')) \, \deg v \\
&= -\sum_{v \in V_0 \cup N} \min(0, v(f') - v(f) + v(h) - v(h')) \, \deg v \\
&= -\sum_{p | v(h), p | v(f)} \min(0, v(f') - v(f) + v(h) - v(h')) \, \deg v \\
&\quad -\sum_{p | v(h), p \nmid v(f)} \min(0, v(f') - v(f) + v(h) - v(h')) \, \deg v \\
&\leq -\sum_{p | v(h)} \min(0, v(h) - v(h')) \, \deg v - \sum_{p | v(h), p \nmid v(f)} (-1) \, \deg v \\
&\leq \sum_{p | v(h), p \nmid v(f)} \deg v + \sum_{p | v(h)} (v(h') - v(h)) \, \deg v \\
&= \sum_{p | v(h), p \nmid v(f)} \deg v + 2g - 2 + \sum_{p \nmid v(h)} \deg v \\
&\leq 2g - 2 + \sum_{v \in V_0} \deg v.
\end{aligned} \tag{15}$$

We remark that the application of (3) (needed for the last equation) bases on the assumtion that h is not a p-th power. Since no proper subsum of the γ_i vanishes we have $(\gamma_i/\gamma_2)'' \neq 0$ in (13), hence $h = \gamma_1/\gamma_2$ cannot be a p-th power.

In view of (13), (12) and the estimate (15) we obtain (9) and (8). □

Remark 1 Splitting in K the valuations of $k[t]$ of small degree, we usually obtain far too many possible valuations, for which $\sum \deg v$ exceeds the (usually very small) bound in (11). To speed up further calculations at this stage it is advisable to consider several possible valuation sets N containing just a few valuations, such that the bound in (11) holds. This enables one also to parallelize the calculations.

Remark 2 From the proof of the last Theorem we can easily deduce that

$$\frac{\gamma_i}{\gamma_n} = x_{in} \cdot \Phi_i \quad (i = 1, 3, \ldots, n)$$

with $V_0 \cup N$-units Φ_i, x_{in} subject to

$$x_{1n} + x_{3n} + \ldots + x_{n-1,n} = 1$$

and

$$H(\Phi_i) \leq 2g - 2 + \sum_{v \in V_0} \deg v \ .$$

Hence, the solution of a unit equation in $n-1$ V_0-units is reduced to determining the solutions of a unit equation in $n-2$ $V_0 \cup N$-units.

Remark 3 Assume that $x_{in} \in K^p$. Then for any valuation $v \in N$ (not in V_0) we have

$$v\left(\frac{\gamma_i}{\gamma_n}\right) = v(x_{in}) + v(\Phi_i).$$

Since $v(\gamma_i/\gamma_n) = 0$ and $p|v(x_{in})$, we have $p|v(\Phi_i)$ for all these valuations. In several examples the small bound (8) implies $|v(\Phi_i)| < p$ which in such cases imply that N is in fact empty and both x_{in} and Φ_i are V_0–units. If $|v(\Phi_i)| \geq p$ then it can be used to exclude p-th powers with higher exponents of p.

5 Unit equations in three variables

In this section we develop an explicit method for solving equation (6), respectively (7), in the case $n = 4$.

According to Remark 2 in the previous section, the terms in equation (7) can be expressed as

$$\frac{\gamma_1}{\gamma_4} = x_0\Phi, \quad \frac{\gamma_3}{\gamma_4} = y_0\Psi, \quad \frac{\gamma_2}{\gamma_4} = z_0\Lambda \tag{16}$$

where x_0, y_0 are corresponding solutions of the $V_0 \cup N$-unit equation $x_0 + y_0 = 1$, z_0 is a solution of a similar equation, and the elements Φ, Ψ, Λ are also $V_0 \cup N$-units of small height, that can be considered as fixed elements (we can explicitly determine all their possible values). Therefore equation (7) can be written in the form

$$x_0\Phi + y_0\Psi + z_0\Lambda = -1. \tag{17}$$

We need to consider two cases I and II.

I. If any of the three elements x_0, y_0, z_0, say x_0, is not a p-th power, then we can calculate all potential values of x_0 according to Theorem (4.1). Also, we have $y_0 = 1 - x_0$, and we get z_0 from equation (17).

II. If all these elements are p-th powers, then using local derivation at an arbitrary valuation we get

$$x_0\Phi' + y_0\Psi' + z_0\Lambda' = 0. \tag{18}$$

Note that $x_0' = y_0' = z_0' = 0$ in that case. We need to discuss two subcases (A, B) of II.

A) If $\Phi, \Psi, \Lambda \in k$, then equation (18) is meaningless but both sides of (17) are p-th powers and we can take p-th roots to make the valuations of x_0, y_0, z_0 smaller. This can be applied repeatedly until we end up in case I.

B) If some of Φ, Ψ, Λ are not constants, then using $y_0 = 1 - x_0$ we get

$$\begin{aligned} (\Phi - \Psi)\, x_0 \;+\; \Lambda\, z_0 \quad &= \quad -1 - \Psi \\ (\Phi' - \Psi')\, x_0 \;+\; \Lambda'\, z_0 \quad &= \quad -\Psi'. \end{aligned} \tag{19}$$

From this system of linear equations we can determine x_0 and z_0. Note that the only case when this system of linear equations is not uniquely solvable is when $(\Phi - \Psi)\Lambda' - (\Phi' - \Psi')\Lambda = 0$ that is $(\Phi - \Psi)/\Lambda$ is a constant. In this case we can use a further equation

$$(\Phi'' - \Psi'')\, x_0 \;+\; \Lambda''\, z_0 \;=\; -\Psi''.$$

6 Application to norm form equations

Let L be a finite extension field of K of degree $m \geq 4$ and denote by O_L the integral closure of $k[t]$ in L. Let $\alpha, \beta \in O_L$ be linearly independent over

K such that $L = K(\alpha, \beta)$. Let $0 \neq \mu \in O_K$ and consider the norm form equation in three variables

$$N_{L/K}(x + \alpha y + \beta z) = \mu \quad (x, y, z \in O_K). \tag{20}$$

Denote by α_i, β_i ($i = 1, \ldots, m$) the conjugates of α, β over K. Then for any distinct $1 \leq i, j, k, l \leq m$ the linear forms $\delta_h(X, Y, Z) = X + \alpha_h Y + \beta_h Z$ are linearly dependent over L, hence we can explicitly calculate $\gamma_h \in L$ ($h = i, j, k, l$) such that for any solution $x, y, z \in O_K$ of equation (20) we have

$$\gamma_i \cdot \delta_i(x, y, z) + \gamma_j \cdot \delta_j(x, y, z) + \gamma_k \cdot \delta_k(x, y, z) + \gamma_l \cdot \delta_l(x, y, z) = 0$$

whence

$$-\frac{\gamma_i \cdot \delta_i(x, y, z)}{\gamma_l \cdot \delta_l(x, y, z)} - \frac{\gamma_j \cdot \delta_j(x, y, z)}{\gamma_l \cdot \delta_l(x, y, z)} - \frac{\gamma_k \cdot \delta_k(x, y, z)}{\gamma_l \cdot \delta_l(x, y, z)} = 1.$$

Let V_0 be the set of valuations of L containing the infinite valuations and the valuations occurring in μ. Then all $\delta_i(x, y, z)$ are V_0-units. Let V_1 be an extension of the set V_0 containing also the valuations occurring in any of the $\gamma_h \in L$ ($h = i, j, k, l$). Then all fractions in the above equation are V_1-units and we can apply our results of the previous section. Usually p-th powers can be excluded, if there exist valuations (not contained in V_0) which only occur in γ_i/γ_l with values not divisible by p, but cannot occur in $\delta_i(x, y, z)/\delta_l(x, y, z)$ or by considering Galois automorphisms (see Example 2).

In this way we can calculate elements ν_i such that

$$\delta_i(x, y, z) = \nu_i \cdot \delta_l(x, y, z)$$

for $i = 1, \ldots, m$. Substituting them into equation (20) we get

$$\left(\prod_{i=1}^{m} \nu_i \right) \cdot \delta_l(x, y, z)^m = \mu$$

which makes it possible to determine $\delta_l(x, y, z)$ and then all $\delta_i(x, y, z)$. By solving systems of linear equations we can then determine all possible solutions (x, y, z) of equation (20).

7 Examples

Example 1
Let $k = \mathbb{F}_5$ and let α be a root of

$$z^4 - t = 0.$$

Let $K = k(t)$ and $L = K(\alpha)$ and consider the solutions of the norm form equation

$$N_{L/K}(x + \alpha y + \alpha^2 z) = c \cdot t \quad (x, y, z \in k[t]) \tag{21}$$

with an arbitrary $c \in k^*$.

The field L has genus $g = 0$ and L/K has a cyclic Galois group. The conjugates of α over K are

$$\alpha_1 = \alpha, \ \alpha_2 = 2\alpha, \ \alpha_3 = -\alpha, \ \alpha_4 = -2\alpha.$$

The linear forms $\delta_i(x, y, z) = x + \alpha_i y + \alpha_i^2 z$ satisfy

$$\delta_1(x, y, z) - \delta_2(x, y, z) + \delta_3(x, y, z) - \delta_4(x, y, z) = 0$$

whence

$$\frac{\delta_1(x, y, z)}{\delta_4(x, y, z)} - \frac{\delta_2(x, y, z)}{\delta_4(x, y, z)} + \frac{\delta_3(x, y, z)}{\delta_4(x, y, z)} = 1.$$

There is one infinite valuation v_∞ of degree 1 in L and there is one valuation v_0 of degree 1 corresponding to t. Set $V_0 = V_1 = \{v_\infty, v_0\}$. Since $2g - 2 + \sum_{v \in V_0} \deg v = 0$, the set N of new valuations (those introduced in Theorem 4.1) is empty and in the representation

$$\frac{\delta_1(x, y, z)}{\delta_4(x, y, z)} = x_0 \Phi$$

the solutions x_0 of the V_0-unit equation in two variables and the V_0-units Φ are constants. (Therefore the p-th powers of x_0 are also constants.) Similarly $\delta_1(x, y, z)/\delta_4(x, y, z)$ and $\delta_2(x, y, z)/\delta_4(x, y, z)$ are constants, whence

$$c_1 \cdot \delta_4(x, y, z)^4 = c \cdot t$$

with some $c_1 \in k^*$. This implies $\delta_4(x, y, z) = c_2 \alpha_4$, whence $\delta_i(x, y, z) = c_2 \alpha_i$ $(i = 1, 2, 3)$ with $c_2 \in k^*$. The only solution of equation (21) is $x = 0, y = c, z = 0$ for some $c \in k^*$.

Example 2
Let $k = \mathbb{F}_3$ and let α be a root of

$$z^4 + 2tz^3 + tz + 1 = 0.$$

(Observe that this is in fact the family of simplest quartic fields, cf. [7]).

Let $K = k(t)$ and $L = K(\alpha)$. Consider the solutions of the norm form equation

$$N_{L/K}(x + \alpha y + \alpha^2 z) = c \ \ (x, y, z \in k[t]) \tag{22}$$

with an arbitrary $c \in k^*$. L/K has a cyclic Galois group generated by

$$\sigma(\alpha) = \frac{\alpha - 1}{\alpha + 1}.$$

Let $\alpha_i = \sigma^{i-1}(\alpha)$ for $i = 1, 2, 3, 4$. The linear forms $\delta_i(x, y, z) = x + \alpha_i y + \alpha_i^2 z$ satisfy

$$\varepsilon\, \delta_1(x, y, z) + \eta\, \delta_2(x, y, z) + \rho\, \delta_3(x, y, z) = \delta_4(x, y, z) \tag{23}$$

with certain units ε, η, ρ which are easy to calculate.

The function field L has genus $g = 0$, it has four infinite valuations $v_{\infty,1}, v_{\infty,2}, v_{\infty,3}, v_{\infty,4}$ all of degree 1. By our notation $V_0 = \{v_{\infty,1}, v_{\infty,2}, v_{\infty,3}, v_{\infty,4}\}$, then all summands in equation (23) are V_0-units.

We have $2g-2+\sum_{v\in V_0} \deg v = 2$. For the set of new valuations N (those introduced in Theorem 4.1) we have $\sum_{v\in N} \deg v \leq 2$. Factorizing $t^{3^2} - t$ over k we find that apart from the infinite valuations all valuations have degrees at least two. Moreover, the only valuations of degree 2 are the two valuations $v_{0,1}, v_{0,2}$ corresponding to t and the valuation v_2 corresponding to t^2+1. Hence the set N contains exactly one of the above three valuations of degree 2.

Up to constant factors there are 115 $V_0 \cup N$-units Φ of height ≤ 2 and there are 664 solutions of the $V_0 \cup N$-unit equation $x_0 + y_0 = 0$ of height ≤ 4 which are not pth powers. Applying Theorem 4.1 to the equation

$$\varepsilon \frac{\delta_1(x, y, z)}{\delta_4(x, y, z)} + \eta\, \frac{\delta_2(x, y, z)}{\delta_4(x, y, z)} + \rho\, \frac{\delta_3(x, y, z)}{\delta_4(x, y, z)} = 1$$

we obtain

$$\frac{\eta\, \delta_2(x, y, z)}{\varepsilon\, \delta_1(x, y, z)} = x_0^{p^\kappa}\, \Phi$$

where x_0, Φ is as above, p^κ is an unknown exponent. By Remark 2 after Theorem 4.1 we also have

$$\frac{\rho\,\delta_3(x,y,z)}{\varepsilon\,\delta_1(x,y,z)} = y_0^{p^\kappa}\,\Psi$$

where $y_0 = 1 - x_0$ is the corresponding solution of the $V_0 \cup N$-unit equation $x_0 + y_0 = 0$, and Ψ is a $V_0 \cup N$-unit of height $H(\Psi) \leq 2$.

This yields

$$\frac{\delta_1(x,y,z)}{\delta_2(x,y,z)} = \frac{\mu}{x_0^{p^\kappa}}, \tag{24}$$

$$\frac{\delta_1(x,y,z)}{\delta_3(x,y,z)} = \frac{\nu}{y_0^{p^\kappa}}, \tag{25}$$

with

$$\mu = \frac{\eta}{\varepsilon\Phi}, \quad \nu = \frac{\rho}{\varepsilon\Psi}.$$

Applying σ to (24) we get

$$\frac{\delta_2(x,y,z)}{\delta_3(x,y,z)} = \frac{\sigma(\mu)}{\sigma(x_0)^{p^\kappa}}$$

whence using (24) again we obtain

$$\frac{\delta_1(x,y,z)}{\delta_3(x,y,z)} = \frac{\mu\,\sigma(\mu)}{x_0^{p^\kappa}\;\sigma(x_0)^{p^\kappa}}.$$

This, compared with (25) implies

$$\frac{\mu\,\sigma(\mu)}{x_0^{p^\kappa}\;\sigma(x_0)^{p^\kappa}} = \frac{\nu}{y_0^{p^\kappa}},$$

that is

$$\left(\frac{1-x_0}{x_0\,\sigma(x_0)}\right)^{p^\kappa} = \frac{\nu}{\mu\,\sigma(\mu)}.$$

The right hand side of this equation is of bounded height. If the left hand side is not constant, then by comparing heights, this equation allows to bound the exponent p^κ. Indeed, apart from 9 possible solutions x_0, the left hand side is not constant and considering all possible values of Φ, Ψ we obtain $\kappa \leq 1$.

In order to exclude pth powers of x_0 in the remaining 9 cases consider the $V_0 \cup N$-unit equation

$$-\frac{\varepsilon\,\delta_1(x,y,z)}{\rho\,\delta_3(x,y,z)} - \frac{\eta\,\delta_2(x,y,z)}{\rho\,\delta_3(x,y,z)} + \frac{\delta_4(x,y,z)}{\rho\,\delta_3(x,y,z)} = 1.$$

Similarly as above we become

$$\frac{\eta\,\delta_2(x,y,z)}{\varepsilon\,\delta_1(x,y,z)} = x_0^{p^\kappa}\,\Phi \tag{26}$$

and

$$\frac{\delta_4(x,y,z)}{\varepsilon\,\delta_1(x,y,z)} = y_0^{p^\kappa}\,\Psi \tag{27}$$

where again we have the same possibilities for the values of $x_0, y_0 = 1 - x_0, \Psi, \Phi$. Applying σ to equation (27) yields

$$\frac{\delta_1(x,y,z)}{\delta_2(x,y,z)} = \sigma(\varepsilon)\,\sigma(y_0)^{p^\kappa}\,\sigma(\Psi),$$

which, compared with equation (26) implies

$$\sigma(\varepsilon)\,\sigma(y_0)^{p^\kappa}\,\sigma(\Psi) = \frac{\eta}{\varepsilon\,x_0^{p^\kappa}\,\Phi},$$

that is

$$(x_0\,\sigma(1-x_0))^{p^\kappa} = \frac{\eta}{\varepsilon\,\sigma(\varepsilon)\Phi\,\sigma(\Psi)}.$$

Comparing again heights on both sides of the last equation we usually get $\kappa \leq 1$ and we can exclude pth powers for all remaining $x_0 \notin k^*$. For $x_0 \in k^*$ (i.e. $x_0 = 2$) the exponent κ is of course arbitrary.

Now we use for example equation (24) to calculate

$$s = \frac{x_0^{p^\kappa}}{\mu}$$

where we consider all possible values of x_0 and Φ (in calculating μ), and $\kappa = 0, 1$. Then we have

$$\begin{aligned} \delta_2(x,y,z) &= s\,\delta_1(x,y,z) \\ \delta_3(x,y,z) &= \sigma(s)\,\delta_2(x,y,z) = s\,\sigma(s)\,\delta_1(x,y,z) \\ \delta_4(x,y,z) &= \sigma^2(s)\,\delta_3(x,y,z) = s\,\sigma(s)\,\sigma^2(s)\,\delta_1(x,y,z), \end{aligned} \tag{28}$$

therefore by the original equation (22) we obtain

$$c = \delta_1(x,y,z)\ \delta_2(x,y,z)\ \delta_3(x,y,z)\ \delta_4(x,y,z) = s^3\ \sigma(s)^2\ \sigma^2(s)\ \delta_1(x,y,z)^4$$

which allows to determine all possible values of $\delta_1(x,y,z)$, whence by (28) we may calculate the values of $\delta_i(x,y,z), i = 2,3,4$, as well. Solving the corresponding systems of linear equations we obtain the following solutions of equation (22):

x	y	z	x	y	z	x	y	z	x	y	z	x	y	z
0	0	1	0	0	2	0	1	0	0	1	1	0	1	2
0	2	0	0	2	1	0	2	2	1	0	0	1	0	2
1	1	0	1	1	1	1	2	0	1	2	1	2	0	0
2	0	1	2	1	0	2	1	2	2	2	0	2	2	2

x	y	z	x	y	z	x	y	z
1	t	1	2	$2t$	t	$t+2$	$t+2$	2
1	t	2	2	$2t$	$2t$	$2t$	1	t
1	t	t	2	$2t+1$	$t+2$	$2t$	t	2
1	t	$2t$	2	$2t+2$	$2t+2$	$2t$	$2t$	1
1	$t+1$	$t+1$	t	2	$2t$	$2t+1$	0	$t+1$
1	$t+2$	$2t+1$	t	t	2	$2t+1$	$2t+1$	1
1	$2t$	1	t	$2t$	1	$2t+2$	0	$t+2$
2	t	2	$t+1$	0	$2t+1$	$2t+2$	$t+1$	2
2	$2t$	1	$t+1$	$2t+2$	1			
2	$2t$	2	$t+2$	0	$2t+2$			

x	y	z	x	y	z
0	t	t^2+2	t^2+2	t^2+2t+2	$2t$
0	$2t$	$2t^2+1$	t^2+2	$2t^2+2t+1$	t
0	t^2+2	$2t$	t^2+t+2	t	$2t^2+t+1$
0	t^2+t+2	t^2+2t+2	t^2+t+2	t^2+2t+2	0
0	t^2+2t+2	$2t^2+2t+1$	t^2+t+2	$2t^2+1$	t^2+2t+2
0	$2t^2+1$	t	t^2+2t+2	t	$2t^2+2t+1$
0	$2t^2+t+1$	t^2+t+2	t^2+2t+2	t^2+2	t^2+t+2
0	$2t^2+2t+1$	$2t^2+t+1$	t^2+2t+2	$2t^2+2t+1$	0
t	t^2+1	$2t$	$2t^2+1$	t	0
t	t^2+2	0	$2t^2+1$	t^2+t+2	$2t$
t	t^2+t+2	t^2+2	$2t^2+1$	$2t^2+t+1$	t
t	t^2+2t+2	$2t^2+1$	$2t^2+2$	t	t^2+1
$2t$	$2t^2+1$	0	$2t^2+t+1$	$2t$	t^2+t+2
$2t$	$2t^2+2$	t	$2t^2+t+1$	t^2+t+2	0
$2t$	$2t^2+t+1$	t^2+2	$2t^2+t+1$	$2t^2+1$	$2t^2+2t+1$
$2t$	$2t^2+2t+1$	$2t^2+1$	$2t^2+2t+1$	$2t$	t^2+2t+2
t^2+1	$2t$	$2t^2+2$	$2t^2+2t+1$	t^2+2	$2t^2+t+1$
t^2+2	$2t$	0	$2t^2+2t+1$	$2t^2+t+1$	0

x	y	z
t^2+1	t^3+2t	$2t^2+2$
$2t^2+2$	$2t^3+t$	t^2+1
t^3+t^2+2t	t^4+2t^3+t+1	$t^4+2t^3+t^2+t+1$
$2t^3+2t^2+t$	$2t^4+t^3+2t+2$	$2t^4+t^3+2t^2+2t+2$
t^3+2t^2+2t	t^4+t^3+2t+1	$2t^4+2t^3+2t^2+t+2$
$2t^3+t^2+t$	$2t^4+2t^3+t+2$	$t^4+t^3+t^2+2t+1$
$2t^3+t$	t^2+1	t^3+2t
t^3+2t	$2t^2+2$	$2t^3+t$
$t^4+2t^3+t^2+t+1$	$2t^4+t^3+2t+2$	t^3+t^2+2t
$2t^4+t^3+2t^2+2t+2$	t^4+2t^3+t+1	$2t^3+2t^2+t$
$t^4+t^3+t^2+2t+1$	t^4+t^3+2t+1	$2t^3+t^2+t$
$2t^4+2t^3+2t^2+t+2$	$2t^4+2t^3+t+2$	t^3+2t^2+2t

Example 3
Let $k=\mathbb{F}_5$ and let α be a root of

$$z^4+(t+3)z^2+1=0.$$

Let $K=k(t)$ and $L=K(\alpha)$. Consider the solutions of the norm form equation

$$N_{L/K}(x+\alpha y+\alpha^2 z)=ct \;\; (x,y,z\in k[t]) \tag{29}$$

with an arbitrary $c\in k^*$. L/K has a bicyclic Galois group. The roots of f are

$$\begin{aligned}
\alpha_1 &= \sqrt{t}+\sqrt{t+1}\\
\alpha_2 &= -\sqrt{t}+\sqrt{t+1}\\
\alpha_3 &= \sqrt{t}-\sqrt{t+1}\\
\alpha_4 &= -\sqrt{t}-\sqrt{t+1}.
\end{aligned}$$

The authomorphism group of L/K is generated by σ_1,σ_2 with

$$\sigma_1(\sqrt{t})=-\sqrt{t},\;\; \sigma_1(\sqrt{t+1})=\sqrt{t+1}$$

and

$$\sigma_2(\sqrt{t})=\sqrt{t},\;\; \sigma_2(\sqrt{t+1})=-\sqrt{t+1}.$$

This implies that the non-trivial elements (all of order two) of the authomorphism group are $\sigma_1,\sigma_2,\sigma_1\sigma_2$ with

$$\sigma_1(\alpha_1)=\alpha_2, \qquad \sigma_1(\alpha_3)=\alpha_4$$

$$\begin{aligned} \sigma_2(\alpha_1) &= \alpha_3, & \sigma_1(\alpha_2) &= \alpha_4 \\ \sigma_1\sigma_2(\alpha_1) &= \alpha_4, & \sigma_1\sigma_2(\alpha_2) &= \alpha_3. \end{aligned}$$

Solving equation (29) we shall use the ideas of Section 5. The linear forms $\delta_i(x,y,z) = x + \alpha_i y + \alpha_i^2 z$ satisfy

$$\delta_1(x,y,z) + 4\alpha_1^2\,\delta_2(x,y,z) + \alpha_1^2\,\delta_3(x,y,z) = \delta_4(x,y,z), \tag{30}$$

hence compared with equation (16) we have

$$\begin{aligned} \frac{\gamma_1}{\gamma_4} &= -\frac{\delta_1(x,y,z)}{\delta_4(x,y,z)} \\ \frac{\gamma_3}{\gamma_4} &= -\alpha_1^3\,\frac{\delta_3(x,y,z)}{\delta_4(x,y,z)} \\ \frac{\gamma_2}{\gamma_4} &= -4\alpha_1^2\,\frac{\delta_2(x,y,z)}{\delta_4(x,y,z)}. \end{aligned} \tag{31}$$

Further, we shall use that

$$\frac{\delta_2(x,y,z)}{\delta_4(x,y,z)} = \frac{\delta_2(x,y,z)}{\delta_3(x,y,z)} \cdot \frac{\delta_3(x,y,z)}{\delta_4(x,y,z)} = \sigma_1\left(\frac{\delta_1(x,y,z)}{\delta_4(x,y,z)}\right) \cdot \frac{\delta_3(x,y,z)}{\delta_4(x,y,z)}. \tag{32}$$

The function field L has genus $g = 0$, it has two infinite valuations $v_{\infty,1}, v_{\infty,2}$ and two valuations $v_{0,1}, v_{0,2}$ corresponting to t, all of degree 1. Let $V_0 = \{v_{\infty,1}, v_{\infty,2}, v_{0,1}, v_{0,2}\}$, then all summands in equation

$$\frac{\gamma_1}{\gamma_4} + \frac{\gamma_2}{\gamma_4} + \frac{\gamma_3}{\gamma_4} = -1 \tag{33}$$

are V_0-units. We have $2g-2+\sum_{v\in V_0} \deg v = 2$. For the set of new valuations N (cf. Theorem 4.1) we have $\sum_{v\in N} \deg v \leq 2$. Factorizing $t^{5^2} - t$ over k and considering elements of bounded height with non-zero values only at given valuations we find that additionally only the valuations $v_{1,1}, v_{1,2}$, corresponding to $t+1$ both of degree 1, may occur in N.

According to (17) we have

$$\frac{\gamma_1}{\gamma_4} = -x_0\Phi, \quad \frac{\gamma_3}{\gamma_4} = -(1-x_0)\Psi, \tag{34}$$

where x_0 and Φ, Ψ are $V_0 \cup N$-units, x_0 satisfying the unit equation $x_0 + y_0 = 1$ with a $V_0 \cup N$-unit y_0, with $H(\Phi), H(\Psi) \leq 2$ and x_0 is either a pth power or $H(x_0) \leq 4$. Further, by (32) we get

$$\frac{\gamma_2}{\gamma_4} = -4\alpha_1^2 \, \frac{\delta_2(x,y,z)}{\delta_4(x,y,z)} = -4\alpha_1^2 \, \sigma_1 \left(\frac{\delta_1(x,y,z)}{\delta_4(x,y,z)} \right) \cdot \frac{\delta_3(x,y,z)}{\delta_4(x,y,z)} =$$

$$= (-4) \, \alpha_1^2 \, \sigma_1 \left(-\frac{\gamma_1}{\gamma_4} \right) \cdot \frac{(-1)}{\alpha_1^3} \cdot \frac{\gamma_3}{\gamma_4} = \left(\frac{-4}{\alpha_1} \right) \, \sigma_1(x_0 \Phi) \, (1 - x_0) \, \Psi. \tag{35}$$

This implies that equation (33) can be written in the form

$$x_0 \Phi \; + \; \left(\frac{-4 \, \sigma_1(\Phi) \, \Psi}{\alpha_1} \right) \, \sigma_1(x_0) \, (1 - x_0) \; + \; (1 - x_0) \, \Psi \; = \; 1 \tag{36}$$

or equivalently

$$x_0 \Phi \; + \; (1 - x_0) \, \Psi \; + \; z_0 \, \Lambda \; = \; 1 \tag{37}$$

with

$$\Lambda \; = \; \frac{-4 \, \sigma_1(\Phi) \, \Psi}{\alpha_1}, \quad z_0 \; = \; \sigma_1(x_0) \, (1 - x_0).$$

I. If x_0 is a pth power then by $H(\Phi) \leq 2 < p$ Remark 3 after Theorem 4.1 implies that N is in fact empty, and x_0, Φ, Ψ are V_0 units. Obviously $1 - x_0$ and $z_0 = \sigma_1(x_0)(1 - x_0)$ are also pth powers. Using local derivation at a valuation by Section 5 equation (37) gives

$$\begin{aligned} (\Phi - \Psi) \, x_0 \; + \; \Lambda \, z_0 \; &= \; 1 - \Psi \\ (\Phi' - \Psi') \, x_0 \; + \; \Lambda' \, z_0 \; &= \; -\Psi'. \end{aligned} \tag{38}$$

Up to constant factors there are 55 V_0 units of height ≤ 2. Observe that $\Phi = \Psi$ is not possible and eliminate z_0 from the above system of equations to get

$$x_0 (\Lambda' (\Phi - \Psi) - \Lambda (\Phi' - \Psi')) \; = \; \Lambda' (1 - \Psi) + \Lambda \Psi'.$$

Considering all possible values for Φ and Ψ we calculated x_0 from the above equation. Note that in all cases when the coefficient of x_0 was zero (that is $(\Phi - \Psi)/\Lambda$ is constant) we had a non-zero right hand side, that is a contradictory equation. We tested if x_0 is indeed a V_0 unit and a pth power. We obtained, that all possible values of x_0 are constants. By equations (31), (34), (35) we can calculate the actual values of $\delta_i(x,y,z)/\delta_4(x,y,z)$ $(i = 1, 2, 3)$. Further, by the original norm form equation (29) we have

$$\delta_4(x,y,z)^4 \; = \; c \cdot t \cdot \left(\frac{\delta_1(x,y,z)}{\delta_4(x,y,z)} \cdot \frac{\delta_2(x,y,z)}{\delta_4(x,y,z)} \cdot \frac{\delta_3(x,y,z)}{\delta_4(x,y,z)} \right)^{-1}$$

which gives $\delta_4(x,y,z)$, whence we can calculate the values of the other linear forms. By solving a system of linear equations we get x,y,z. All solutions we calculated in this case are

$$(x,y,z) = (1,4,0), (0,4,1), (1,1,0), (0,1,1)$$

and their constant multiples.

II. Assume that x_0 is not a pth power. Then $N = \{v_{1,1}, v_{1,2}\}$. x_0 and Φ, Ψ are $V_0 \cup N$-units with

$$H(x_0) \le 4, \quad H(\Phi) \le 2, \quad H(\Psi) \le 2.$$

There are 271 possible values for x_0 and up to constant factor there are 743 possible values for Φ (and Ψ). To reduce the number of possible cases to test we consider

$$\begin{aligned} 1 &= \frac{\delta_1(x,y,z)}{\delta_4(x,y,z)} \cdot \frac{\delta_4(x,y,z)}{\delta_1(x,y,z)} = (x_0\Phi) \cdot \sigma_1\sigma_2(x_0\Phi) \\ 1 &= \frac{\delta_2(x,y,z)}{\delta_3(x,y,z)} \cdot \frac{\delta_3(x,y,z)}{\delta_2(x,y,z)} = \sigma_1(x_0\Phi) \cdot \sigma_2(x_0\Phi). \end{aligned}$$

Checking the above equations instead of $271 \cdot 743 = 201353$ pairs there only remain 4235 possible pairs x_0, Φ and for each pair we can calculate the possible constant factors of Φ, as well. Further, equation (36) gives the corresponding Ψ which also must be checked if it is a $V_0 \cup N$-unit of height ≤ 2. From x_0, Φ, Ψ we can calculate the solutions x,y,z of equation (29). In this case we do not get any further solutions.

Remark All computations were performed by using Kash [1]. The computations of Example 1 took just a few seconds, Examples 2 and 3 took several minutes.

References

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

[2] J.H.Evertse and K.Győry, *Finiteness criteria for decomposable form equations*, Acta Arith. **50** (1988), 357–379.

[3] I.Gaál, Diophantine equations and power integral bases, Birkhäuser, Boston, 2002.

[4] I.Gaál and M.Pohst, *Diophantine equations over global function fields I: The Thue equation*, J.Number Theory **119**(2006), 49–65.

[5] I.Gaál and M.Pohst, *Diophantine equations over global function fields II: S-integral solutions of Thue equations*, Experimental Math., **15**(2006), No.1., 1–6.

[6] I.Gaál and M.Pohst, *Diophantine equations over global function fields III: An application to resultant form equations*, submitted.

[7] M.N.Gras, *Table numerique du nombre de classes et des unites des extensions cycliques reelles de degre 4 in Q*, Publ. Math. Fac. Sci. Besancon, 1977-1978, fasc. 2.

[8] I.Járási, *Computing small solutions of unit equations in three variables I: Application to norm form equations*, submitted, *II: Resultant form equations*, Publ. Math. (Debrecen), **65**(2004), 399–408.

[9] R.C.Mason, Diophantine equations over function fields, Cambridge University Press, 1984.

[10] R.C.Mason, *Norm form equations I*, J. Number Theory **22**(1986), 190–207.

[11] R.C.Mason, *Norm form equations III: Positive characteristic*, Math. Proc. Camb. Philos. Soc. **99** (1986), 409–423.