J. Math. Crypt. **3** (2009), 237–248

DOI 10.1515 / JMC.2009.014

On solving norm equations in global function fields

István Gaál and Michael E. Pohst

Communicated by Jaime Gutierrez

Abstract. The potential of solving norm equations is crucial for a variety of applications of algebraic number theory, especially in cryptography. In this article we develop general effective methods for that task in global function fields for the first time.

Keywords. Norm equations, unit equations, global function fields.

AMS classification. 11Y50, 11T71, 11D57.

1 Introduction

Let E/F be a (finite) extension of fields of degree d. Let $\omega_1, \ldots, \omega_d$ be a fixed F-basis of E. Then each element $x \in E$ has a presentation

$$x(\omega_1, \ldots, \omega_d) = (\omega_1, \ldots, \omega_d)M_x$$

with a matrix $M_x \in F^{d \times d}$. The determinant $\det(M_x)$ is called the *norm* $N(x)$ of the element $x \in E$ with respect to F. Since $N(x)$ is – up to sign – the constant term in the characteristic polynomial of x it is independent of the choice of the basis.

The calculation of elements of prescribed norm is an important task in algebraic number theory.

From now on, we consider the situation in which the base field F is either the field of rationals $\mathbb{Q}$ or a rational function field $k(t)$ over a finite field $k = \mathbb{F}_q$ of characteristic p, say with $q = p^\ell$. Let o_F be the ring of integers of F, i.e. $\mathbb{Z}$ or $k[t]$, respectively.

The extension E of F is assumed to be separably generated by an element y with minimal polynomial $\underline{m}_y(T) \in o_F[T]$. Then there are d different embeddings of E into the algebraic closure $\overline{F}$, say $\sigma_1, \ldots, \sigma_d$. It can be easily shown that

$$N(x) = \prod_{j=1}^{d} \sigma_j(x) \quad \forall x \in E\,.$$

In the context of global fields, norm equations are in general discussed as follows. We choose $2 \leq m \leq d$ F-linearly independent elements $\gamma_1, \ldots, \gamma_m$ of E, usually in o_E, the integral closure of o_F in E.

Then $M = \oplus_{i=1}^{m} o_F \gamma_i$ is a free o_F-module in E. We are going to look for solutions of

$$N(x) = c \quad (x \in M)$$

Research of first author supported by K67580 and T048791 from the Hungarian National Foundation for Scientific Research

for given c of o_F. Writing $x = x_1\gamma_1 + \cdots + x_m\gamma_m$ with $x_i \in o_F$, the norm $N(x)$ becomes a form in the x_i with coefficients in F.

For two special values of m the computation of solutions is quite well understood. The first one is $m = d$ and the module M is an order of E. This means that the unit group U_M of M operates on M. If there is a solution of $N(x) = c$ then also $x\varepsilon$ is one for any $\varepsilon \in U_M$ of norm 1.

Multiplying x with a suitable ε, we can impose conditions on the *conjugates* $\sigma_j(x)$. All elements of M satisfying those conditions can then be calculated by reduction theory. These ideas are well known for algebraic number fields, see [3], [11], for example. For global function fields the reduction procedure is more subtle because there does not exist an analogue of the LLL-algorithm. We discuss that reduction procedure in Section 3.

We note that both methods require the computation of a set of generators of U_E, the unit group of o_E. The latter is possible with KANT or Magma, for example. (In the number field case also by Pari, of course.)

The second well understood case is $m = 2$ and $d > 2$. In this situation $N(x)$ becomes a binary form and $N(x) = c$ a so-called *Thue*-equation. It can be reduced to a unit equation in two unknowns as follows. For simplicity's sake we assume $\gamma_1 = 1$, $\gamma_2 = \alpha$, hence $x = x_1 + x_2\alpha$. Then we have Siegel's identity:

$$(\sigma_i(\alpha) - \sigma_j(\alpha))\sigma_k(x) + (\sigma_j(\alpha) - \sigma_k(\alpha))\sigma_i(x) + (\sigma_k(\alpha) - \sigma_i(\alpha))\sigma_j(x) = 0$$

for any three pairwise different indices $1 \leq i, j, k \leq d$. Dividing by the last summand, we obtain

$$\frac{(\sigma_i(\alpha) - \sigma_j(\alpha))\sigma_k(x)}{(\sigma_i(\alpha) - \sigma_k(\alpha))\sigma_j(x)} + \frac{(\sigma_j(\alpha) - \sigma_k(\alpha))\sigma_i(x)}{(\sigma_i(\alpha) - \sigma_k(\alpha))\sigma_j(x)} = 1\,.$$

The last equation becomes an S-unit equation $u_1 + u_2 = 1$ by writing $x = \mu\varepsilon$ with $\varepsilon \in U_E$ and $\mu \in o_E$ from a finite set of non-associate solutions of $N(\mu) = c$. (Note that S-units are defined at the beginning of the next section.)

In the number field case one uses Baker type results on linear forms in logarithms, reduction theory and refined enumeration strategies for computing solutions. The fastest algorithm known is that of Bilu and Hanrot [1]. The function field case is discussed in detail in [5]. We just sketch the method below.

According to our present knowledge the resolution of unit equations in more than two variables is needed for solving norm equations in $2 < m < d$ variables. It is not known how to do this in number fields. Therefore it is somewhat surprising that a resolution is still possible in function fields. In [6] we considered the case $m = 3$ which we now generalize to arbitrary m. Also, the case $m = d$ will shortly be treated since we came up with some improvements over the known methods. We conclude with a small illustrative example.

In recent years, the construction of elliptic curves suitable for pairings has attracted increasing interest. The construction of Weil numbers in CM-fields, suitable for pairings, leads to systems of diophantine equations. In a current project we will apply the methods of this paper to obtain solutions in integers as well as polynomials.

2 Global fields: unit equations

Unit equations of type

$$u_1 + \cdots + u_n \ = \ 1\,,$$

where the u_i are elements in a unit group of a function field, play an essential role in the theory and in applications of diophantine equations. We introduce several important notations.

Let $k = \mathbb{F}_q$ be a finite field with $q = p^\ell$ elements. Let E be a finite extension of the rational function field $F = k(t)$ of degree d and genus g. The integral closure of $k[t]$ in E is denoted by o_E. We assume that E is separably generated over $k(t)$ by an element $y \in o_E$ and that k is the full constant field of E.

Any element $f \in E$ has a unique presentation

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

Conjugates of elements (fields) are denoted by upper case indices, i.e. we write $x^{(j)}$ for $\sigma_j(x)$ and $E^{(j)}$ for $\sigma_j(E)$. Let

$$A := \left((y^{(j)})^{i-1}\right)_{1 \le i,j \le d} \in \overline{E}^{\,d \times d}$$

have determinant D. Since E is separably generated we have $D \neq 0$.

From the system of linear equations

$$(f^{(1)}, \ldots, f^{(d)}) \ = \ (h_1, \ldots, h_d)\,A$$

we conclude that the h_i are rational functions in the $f^{(j)}, (y^{(j)})^{i-1}$.

The set of all (exponential) *valuations* of E is denoted by V, the subset of infinite valuations by V_∞. We write $\deg v$ for the degree of the divisor belonging to the valuation $v \in V$. For a non-zero element $f \in E$ the value of f at v is denoted by $v(f)$. 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. The normalized valuations $v_N(f) = v(f)\ \deg v$ satisfy the *product formula*:

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

The *height* of a non-zero element f of E is defined via

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

Because of the product formula this is tantamount to

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

Let V_0 be a finite subset of V. We then consider the V_0-*units* $\gamma \in E$ with $v(\gamma) = 0$ for all $v \notin V_0$.

As we saw in the introduction, the resolution of various Diophantine equations, for example, Thue equations, can often be reduced to that of equations of the form

$$\gamma_1 + \gamma_2 + \gamma_3 = 0\,,$$

where the γ_i are V_0-units for a suitable set V_0. We excerpt the following crucial lemma from [4].

Lemma 2.1. *Let V_0 be a finite subset of V and let γ_i $(1 \le i \le 3)$ be V_0-units the sum of which equals* 0. *Then either $\frac{\gamma_1}{\gamma_3}$ is in E^p or its height is bounded:*

$$H\Big(\frac{\gamma_1}{\gamma_3}\Big) \le 2g - 2 + \sum_{v \in V_0} \deg v\,.$$

Setting $\Phi = -\gamma_1/\gamma_3,\ \Psi = -\gamma_2/\gamma_3$, we obtain a *unit equation in two variables*

$$\Phi + \Psi = 1\,,$$

with V_0-units Φ, Ψ. Because of the characteristic p the number of solutions of such a unit equation is in general infinite.

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

The subsequent corollary shows that for any finite subset V_0 of V the group of V_0-units of E contains only a finite number, say σ, of V_0-units η which are not p^τth powers and for which also $1-\eta$ is a V_0-unit. We denote the set of these units by $\{\eta_1, \ldots, \eta_\sigma\}$.

Corollary 2.2. *Let V_0 be a finite subset of V. We assume that a V_0-unit Φ in E is a solution of a unit equation in two variables. If Φ is not a p^τth power of an element η_i $(1 \le i \le \sigma,\ \tau \in \mathbb{Z}^{>0})$, then Φ belongs to a finite subset of E which can be effectively calculated.*

For the proof we refer to [7, Page 98, Lemma 11]. The proof starts by assuming that Φ is not a pth power in K and therefore also provides the means to calculate the η_i. For an example of a Thue equation with infinitely many solutions see [5].

Next we consider unit equations in more than two variables. Again, V_0 denotes a finite subset of V containing the infinite valuations. Let γ_i $(1 \le i \le n)$ be V_0-units. The equation

$$\gamma_1 + \ldots + \gamma_n = 0 \tag{2.1}$$

is equivalent to the unit equation

$$\Big(-\frac{\gamma_1}{\gamma_n}\Big) + \cdots + \Big(-\frac{\gamma_{n-1}}{\gamma_n}\Big) = 1 \tag{2.2}$$

in $n-1$ variables. We note that we only need to postulate that all fractions in the last equation must be V_0-units.

Those unit equations are of importance since several well-known Diophantine equations (e.g. norm form equations) can be reduced to unit equations in more than two variables. From the results in [6] we easily deduce the following theorem.

Theorem 2.3. *Let V_0 be a finite subset of V and let γ_i $(1 \le i \le n)$ be V_0-units satisfying* (2.1). *Assume that no proper subsum of the sum in* (2.1) *vanishes. Then we can explicitly construct a finite subset N of V, such that*

$$\frac{\gamma_i}{\gamma_n} = x_{in} \cdot \Phi_i \,, \tag{2.3}$$

where x_{in} is a solution of a unit equation

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

with $V_0 \cup N$-units x_{in} $(i = 1, 3, \ldots, n-1)$, and a $V_0 \cup N$-unit Φ_i satisfying

$$H(\Phi_i) \le 2g - 2 + \sum_{v \in V_0} \deg v \,. \tag{2.4}$$

Hence, the solution of a unit equation in $n-1$ V_0-units is reduced to determining the solutions of unit equations in $n-2$ $V_0 \cup N$-units. In [6] only the case $n = 4$ was considered. The generalization to arbitrary n is done here for the first time.

If we replace the γ_i/γ_n in the original unit equation (2.2) via (2.3), then we get

$$\sum_{\substack{i=1 \\ i \ne 2}}^{n-1} x_{in}\Phi_i = -1 \,. \tag{2.5}$$

We need to consider several cases. The main ingredient is to deduce solutions of unit equations from those of unit equations in fewer variables. We remark that this discussion does not include the case in which all x_{in}, Φ_i are in k (compare also the premises in Theorem 2.3).

I. If any of the elements x_{in} $(i = 1, 3, \ldots, n-1)$, say x_{1n}, is not a pth power, then they are obtained from a finite set of solutions of an S-unit equation in $n-2$ variables (compare Theorem 2.3). Also, the $\Phi_1, \ldots, \Phi_{n-1}$ can attain only finitely many values by that theorem. This reduction needs to be carried out until we get unit equations in at most 3 variables, a case which is already treated in [6].

II. If all x_{in} $(i = 1, 3, \ldots, n-1)$ are pth powers, then using local derivation at an arbitrary valuation we get from (2.5) equations

$$\sum_{\substack{i=1 \\ i \ne 2}}^{n-1} x_{in}\Phi_i^{[j]} = 0 \quad (j \in \mathbb{N}) \,, \tag{2.6}$$

where $\Phi_i^{[j]}$ denotes the jth derivative of Φ_i. We note that the derivatives of the x_{in} vanish in this case. We need to discuss subcases (A), (B).

(A) If all Φ_i $(i = 1, 3, \ldots, n-1)$ are pth powers (especially, if they all are in k), then equation (2.6) is meaningless but both sides of (2.5) are pth powers and we can take pth roots to make the valuations of the x_{in}, Φ_i smaller. This can be applied repeatedly until we end up in case I.

(B) Without loss of generality, we assume $\Phi_1 \notin k$ with $\Phi_1^{[1]} \neq 0$. Because of our assumption, in this case we have at least one index $\mu > 1$ with $\Phi_\mu^{[1]} \neq 0$. We compute equations (2.6) for $j = 1, 2, \ldots$ and obtain a linear system of equations for the x_{in}. If there are $n-2$ independent equations for the x_{in} then that system has only the trivial solution and there does not exist a solution of (2.5) for this case. Otherwise, those equations can be used for eliminating variables. We end up in case II but with fewer variables.

3 Application to norm form equations

As before, let E be a finite extension field of $F = k(t)$ of degree $d \geq 3$ and denote by o_E the integral closure of $k[t]$ in E. Then o_E has an o_F-basis (*integral basis*), say $\alpha_1, \ldots, \alpha_d$.

3.1 Norms from o_E

This subsection improves the results of [10]. In that thesis the reduction theory of W. Schmidt in characteristic 0 was generalized to arbitrary characteristics. However, the case when the infinite prime is wildly ramified remained open. In [8] we also showed how to treat that case. Here, we shortly discuss the whole reduction procedure.

Let $\alpha \in o_E$ be a solution of $N_{E/F}(\alpha) = c$ for $c \in o_F$. Then also $\alpha\varepsilon$ is a solution for any unit ε of the unit group U_F with $N_{E/F}(\varepsilon) = 1$. We are therefore only interested in *non-associate* solutions of the original norm equation, i.e. solutions which do not differ by a unit. Scaling such a solution with a power product of the generators of U_E (*fundamental units*) we obtain a solution in an appropriate finite dimensional F-vector space. For this we need a system of fundamental units $\varepsilon_1, \ldots, \varepsilon_{s-1}$ and a *reduced basis* for o_E, where s denotes the number of infinite primes. A system of fundamental units can be computed with Kash or Magma. The full reduction procedure was originally developed in [8]. We sketch the ideas.

We make use of the fact that the non-zero elements v of E admit series expansions (Puiseux series, respectively, Hamburger–Noether series) of the form

$$\Sigma(v) := \sum_{i=m}^{\infty} \phi_i t^{-\nu_i} \tag{3.1}$$

with rational exponents $\nu_m < \nu_{m+1} < \ldots$ and coefficients $\phi_i \in \mathbb{F}_q^\times$. (We note that this is a simplification, in general the ϕ_i may belong to a small finite extension of $\mathbb{F}_q$ of degree e, where e is the least common multiple of the ramification indices of the infinite primes in E.) We need to assume that E over F is separately generated (which can always be achieved by the choice of F). We then have $E = F(y)$ for a suitable element y whose minimal polynomial in $o_F[t]$ has d different zeros. Each zero admits a series expansion so that we obtain a total of d series expansions corresponding to the conjugates of E over F. The isomorphic embeddings of E into the algebraic closure $\overline{F}$ are denoted by $\sigma_1(y), \dots, \sigma_d(y)$, as usual. In each case we obtain an exponential valuation on E via

$$\mathrm{ord} : \mathrm{F} \to \mathbb{Q} : \mathrm{v} \mapsto \begin{cases} \nu_{\mathrm{m}} & \text{for } \mathrm{v} \neq 0, \\ \infty & \text{for } \mathrm{v} = 0. \end{cases} \tag{3.2}$$

We denote the exponential valuations belonging to $\sigma_1, \dots, \sigma_d$ by $\mathrm{ord}_1, \dots, \mathrm{ord}_\mathrm{d}$, respectively.

Now let $\mathbf{B} = \{v_1, \dots, v_d\}$ be a basis of a non-zero ideal $\mathbf{A}$ of o_E. We denote by $\mathbf{v}_j = (v_{ij})_{1 \leq i \leq d}$ the vector whose components v_{ij} are the d series expansions $\sigma_i(v_j)$ $(1 \leq i \leq d)$. We set

$$\mathrm{ord}(\mathbf{v}_\mathrm{j}) := \min \left\{ \mathrm{ord}_\mathrm{i}(\mathrm{v}_{\mathrm{ij}}) : 1 \leq \mathrm{i} \leq \mathrm{d} \right\} =: \nu_\mathrm{j} \,.$$

For each basis element v_j we therefore obtain a vector $\mathbf{\Phi}_j = (\phi_{ij})_{1 \leq i \leq d}$ of coefficients of the leading term of the series expansions, i.e. ϕ_{ij} is the coefficient of $t^{-\nu_j}$ in the expansion $\sigma_i(v_j)$.

We then set

$$\mathrm{ord}(\mathbf{A}) := \mathrm{ord}\Big(\det \Big((\mathrm{v}_{\mathrm{ij}})_{1 \leq \mathrm{i,j} \leq \mathrm{d}} \Big) \Big)$$

(in the sense of (3.2)) and

$$\psi(\mathbf{B}) := \mathrm{ord}(\mathbf{A}) - \sum_{\mathrm{j}=1}^{\mathrm{d}} \mathrm{ord}(\mathbf{v_j}) \,.$$

The basis $\mathbf{B}$ is called *reduced* if the non-negative value $\psi(\mathbf{B})$ vanishes. We have

Lemma 3.1. *An ideal basis $\mathbf{B} = \{v_1, \dots, v_d\}$ of an ideal $\mathbf{A}$ is reduced if and only if for all $(f_1, \dots, f_d) \in \mathbb{F}_q[t]^n$,*

$$\mathrm{ord}\Big(\sum_{\mathrm{i}=1}^{\mathrm{d}} \mathrm{f_i v_i} \Big) = \min_{1 \leq \mathrm{i} \leq \mathrm{d}} \mathrm{ord}(\mathrm{f_i v_i}) \,.$$

If a basis $\{v_1, \dots, v_d\}$ of an ideal $\mathbf{A}$ is reduced and ordered subject to $-\mathrm{ord}(\mathrm{v}_1) \leq -\mathrm{ord}(\mathrm{v}_2) \leq \ldots \leq -\mathrm{ord}(\mathrm{v_d})$, then the values $-\mathrm{ord}(\mathrm{v_i})$ are the successive minima of the ideal $\mathbf{A}$.

In [8] we developed an algorithm for computing a reduced basis which runs in polynomial time in the input data.

From now on, we stipulate that we know a reduced basis $\omega_1, \dots, \omega_d$ of o_E. It is of importance for calculating fundamental units of E [10] and of elements of bounded *maximum norm* (see below) which we need for calculating a maximal set of non-associate solutions of $N_{E/F}(\alpha) = c$ for $c \in o_F$.

In the following, the places of F are denoted by lower case boldface letters, those of E by upper case boldface letters. The infinite place of F which corresponds to the degree valuation is written as $\mathbf{p}_\infty$. For $\mathbf{P}|\mathbf{p}$ the integers $e_{\mathbf{P}|\mathbf{p}}$, $f_{\mathbf{P}|\mathbf{p}}$ and $n_{\mathbf{P}|\mathbf{p}} = e_{\mathbf{P}|\mathbf{p}} f_{\mathbf{P}|\mathbf{p}}$ denote the ramification index, the residue class degree and the local degree, respectively. $N(\mathbf{P})$ is the number of elements in the residue class field of $\mathbf{P}$. The exponential valuation belonging to $\mathbf{P}$ is denoted by $\nu_{\mathbf{P}}$. For every element $f \in E$ we then set

$$|f|_{\mathbf{P}} := N(\mathbf{P})^{-\nu_{\mathbf{P}}(f)/n_{\mathbf{P}|\mathbf{p}}}\,.$$

This normalization has the effect that $|\cdot|_{\mathbf{P}}$ is a prolongation of $|\cdot|_{\mathbf{p}}$ and that the product formula is still valid.

Definition 3.2. The maximum norm of an element $f \in E$ is defined by

$$\|f\|_\infty := \max_{\mathbf{P}|\mathbf{p}_\infty} |f|_{\mathbf{P}}\,.$$

We note that according to [10] a reduced basis $\omega_1, \dots, \omega_d$ of o_E satisfies

$$\|f\|_\infty = \max\left\{|\lambda_i|_\infty \|\omega_i\|_\infty \,:\, 1 \le i \le n\right\}$$

for any $f = \sum_{i=1}^d \lambda_i \omega_i \in o_E$. (This is the analogue of the previous lemma.)

We want to compute a full set of non-associate solutions of $N_{E/F}(\alpha) = c$ for $c \in o_F$. We improve the known methods for number fields and adapt them to the function field case. For number fields the conjugates $\alpha^{(j)}$ of a solution α of $N_{E/F}(\alpha) = |c|$ satisfy

$$\log\left|\frac{\alpha^{(j)}}{c^{1/n}}\right| = \sum_{i=1}^r x_i \log|\varepsilon_i^{(j)}| \quad (x_i \in \mathbb{R},\ 1 \le j \le d)$$

for a full set of fundamental units $\varepsilon_1, \dots, \varepsilon_r$ of o_E. (We note that $r = s-1$ and that a full set of independent units suffices.) In the function field case we let $\mathbf{P}$ be one of the infinite primes of E and obtain for a solution α of $N_{E/F}(\alpha) = c\mu$ for arbitrary $\mu \in k$ analogously

$$\nu_{\mathbf{P}}(\alpha) = \sum_{i=1}^r x_i \nu_{\mathbf{P}}(\varepsilon_i) + \frac{1}{d}\nu_{\mathbf{P}}(c)\,.$$

We note that the coefficients x_i are independent from the choice of $\mathbf{P}|\mathbf{p}$. Substituting α by an associate element just changes the coefficients x_i by rational integers. Such a substitution is supposed to yield small bounds B for $\log\left|\frac{\alpha^{(j)}}{c^{1/n}}\right|$, respectively for

$$|\alpha|_{\mathbf{P}} = N(\mathbf{P})^{-\frac{\nu_{\mathbf{P}}(\alpha)}{n_{\mathbf{P}|\mathbf{p}}}}$$

and hence for $\|\alpha\|_\infty$. This amounts to calculate the maximum distance of an element in the fundamental parallelotope of the lattice spanned by the vectors

$$\left(\log|\varepsilon_i^{(j)}|\right)_{1 \le j \le d} \qquad (i = 1, \dots, r)\,,$$

respectively

$$\left(\nu_{\mathbf{P}}(\varepsilon_i)\right)_{\mathbf{P}|\mathbf{p}} \quad (i = 1, \dots, r)\,,$$

to any lattice point. That task does not cause problems in the dimensions r for which independent (fundamental) units can be presently calculated. Knowing B the calculation of the corresponding solutions α of the norm equation is straightforward by the methods in [9], respectively, in the function field case B yields bounds for the height of α.

We note that the methods of this subsection also hold for arbitrary orders of E, not just the maximal order o_E.

3.2 Norms from free modules of degree less than d

We let $2 \leq m < d$ and $\alpha_i \ (i = 1, \ldots, m)$ be F-linearly independent elements of o_E with $E = F(\alpha_1, \ldots, \alpha_m)$. For $0 \neq \mu \in o_F$ we consider the norm form equation in m variables

$$N_{E/F}\left(\sum_{i=1}^{m} x_i \alpha_i\right) = \mu \quad (x_i \in o_F, \ 1 \leq i \leq m)\,. \tag{3.3}$$

We recall that $\alpha_i^{(j)} \ (j = 1, \ldots, d)$ denote the conjugates of α_i over F. For any distinct indices $1 \leq i_1 < i_2 < \ldots < i_m \leq d$, the linear forms

$$\delta_{i_j}(X_1, \ldots, X_m) = \sum_{i=1}^{m} X_i \alpha_i^{(j)}$$

are linearly independent over E. It is easy to calculate $\gamma_{i_j} \in o_E \ (1 \leq j \leq m)$ such that any solution $x_1, \ldots, x_n$ of equation (3.3) satisfies

$$\sum_{j=1}^{m} \gamma_{i_j} \delta_{i_j}(x_1, \ldots, x_m) = 0\,.$$

Dividing by the last summand on the left-hand side, we obtain an S-unit equation in $m-1$ variables:

$$-\sum_{j=1}^{m-1} \frac{\gamma_{i_j} \delta_{i_j}(x_1, \ldots, x_m)}{\gamma_{i_m} \delta_{i_m}(x_1, \ldots, x_m)} = 1\,. \tag{3.4}$$

Let V_0 be the set of valuations of E containing the infinite valuations and the valuations occurring in μ. Then all $\delta_{i_j}(x_1, \ldots, x_m)$ are V_0-units. Let V_1 be an extension of the set V_0 containing also the valuations occurring in any of the $\gamma_{i_j} \in E \ (j = 1, \ldots, m)$. Then all fractions in equation (3.4) are V_1-units and we can apply the results of the previous section. Usually pth powers can be excluded if there exist valuations (not contained in V_0) which only occur in $\gamma_{i_j}/\gamma_{i_m}$ with values not divisible by p, but cannot occur in $\delta_{i_j}(x_1, \ldots, x_m)/\delta_{i_m}(x_1, \ldots, x_n)$ or by considering Galois automorphisms (see [6]).

In this way we can calculate elements ν_{i_j} such that

$$\delta_{i_j}(x_1, \ldots, x_m) = \nu_{i_j} \delta_{i_m}(x_1, \ldots, x_m)$$

for $j = 1, \dots, m$. Substituting them into equation (3.3), we get

$$\left(\prod_{j=1}^{m} \nu_{i_j}\right) \delta_{i_m}(x_1, \dots, x_m)^m \;=\; \mu\,,$$

from which we calculate $\delta_{i_m}(x_1, \dots, x_m)$ and subsequently all $\delta_{i_j}(x_1, \dots, x_m)$. By solving systems of linear equations, we can then determine all possible solutions $(x_1, \dots, x_m)$ of equation (3.3).

Remark. We note that increasing the number of variables in the unit equation makes our procedure less efficient since the number of valuations usually increases drastically. The amount of calculations to be performed grows roughly exponential with the growth of the number of variables in the unit equation (see the construction in Theorem 2.3).

4 Example

Let $k = \mathbb{F}_5$ and let $\alpha = \alpha_1$ be a root of

$$p(z) = z^5 - z - t = 0\,.$$

Let $E = k(t)(\alpha)$ and denote by o_E the integral closure of $k[t]$ in E. The field E has genus $g = 0$. This field is a Galois (*Artin–Schreier*) extension, the cyclic Galois group is generated by σ:

$$\alpha_{i+1} = \sigma(\alpha_i) = \alpha_i + 1 \quad (i = 1, 2, 3, 4)\,.$$

Let r be a non-zero constant (in k) and consider the solutions of the equation

$$\mathrm{N}_{E/k(t)}(x_1 + \alpha x_2 + \alpha^2 x_3 + \alpha^3 x_4 + \alpha^4 x_5) = r \quad \text{in } \; x_1, x_2, x_3, x_4, x_5 \in k[t]\,. \tag{4.1}$$

Set $\ell_i(\underline{x}) = x_1 + \alpha_i x_2 + \alpha_i^2 x_3 + \alpha_i^3 x_4 + \alpha_i^4 x_5$, then we have the identity

$$\ell_1(\underline{x}) + \ell_2(\underline{x}) + \ell_3(\underline{x}) + \ell_4(\underline{x}) + \ell_5(\underline{x}) = 0\,.$$

The function field E has one infinite valuation v_∞ of degree 1. Let $V_0 = \{v_\infty\}$. Then for any solution $\underline{x} = (x_1, x_2, x_3, x_4, x_5) \in (k[t])^5$ of equation (4.1), the terms in

$$-\frac{\ell_1(\underline{x})}{\ell_5(\underline{x})} - \frac{\ell_2(\underline{x})}{\ell_5(\underline{x})} - \frac{\ell_3(\underline{x})}{\ell_5(\underline{x})} - \frac{\ell_4(\underline{x})}{\ell_5(\underline{x})} = 1$$

are V_0-units. (We note that in case of zero subsums we still get the same solutions.)

By [6] we have

$$\frac{\ell_i(\underline{x})}{\ell_5(\underline{x})} = x_i \cdot \Phi_i\,,$$

where x_i, Φ_i are $V_0 \cup N_1$-units,

$$x_1 + x_2 + x_3 = 1\,, \tag{4.2}$$

and

$$H(\Phi_i) \le 2g - 2 + \sum_{v \in V_0 \cup N_1} \deg v \,.$$

Constructing the set of valuations N_1, we find that $\sum_{v \in N_1} \deg v$ can be estimated from above (see [6]) by

$$2g - 2 + \sum_{v \in V_0} \deg v = -1 \,,$$

hence N_1 is empty. Therefore x_i, Φ_i are V_0-units, and by $H(\Phi_i) = 0$ the Φ_i are constants.

We describe now the solutions of (4.2). By [6] we have

$$x_i = y_i \cdot \Psi_i \,,$$

where y_i, Ψ_i are $V_0 \cup N_1 \cup N_2$-units, y_1, y_2 are solutions of the unit equation $y_1 + y_2 = 1$ and

$$H(\Psi_i) \le 2g - 2 + \sum_{v \in V_0 \cup N_1 \cup N_2} \deg v \,.$$

The set N_2 of valuations is again empty, since $\sum_{v \in N_2} \deg v$ can be estimated from above by

$$2g - 2 + \sum_{v \in V_0 \cup N_1} \deg v = -1 \,.$$

Therefore, y_i, Ψ_i are V_0-units, and by $H(\Psi_i) = 0$ it follows that the Ψ_i are constants.

Finally, we consider the V_0-unit equation in two variables $y_1 + y_2 = 1$. The solutions either satisfy

$$H(y_i) \le 2g - 2 + \sum_{v \in V_0 \cup N_1 \cup N_2} \deg v = -1$$

or they are powers of such elements. Hence the y_i are also constants.

If all fractions

$$\frac{\ell_i(\underline{x})}{\ell_5(\underline{x})} \quad (i = 1, 2, 3, 4)$$

attain constant values, then by equation (4.1) also $\ell_5(\underline{x})^5$ is a constant, as well as $\ell_5(\underline{x})$. Finally, if all the linear forms

$$\ell_i(\underline{x}) \quad (i = 1, 2, 3, 4, 5)$$

attain constant values, then we get only the solutions $(i, 0, 0, 0, 0)$ with $i = 1, 2, 3, 4$ of equation (4.1).

The calculations were carried out with KANT [2].

Acknowledgments. The authors thank the referees for valuable remarks and suggestions which helped to improve the paper.

References

[1] Yuri Bilu and Guillaume Hanrot, *Solving Thue equations of high degree.*, J. Number Theory 60 (1996), pp. 373–392.

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

[3] C. Fieker, A. Jurk, and M. Pohst, *On solving relative norm equations in algebraic number fields.*, Math. Comput. 66 (1997), pp. 399–410.

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

[5] ______, *Diophantine equations over global function fields. II: R-integral solutions of Thue equations.*, Exp. Math. 15 (2006), pp. 1–6.

[6] ______, *Diophantine equations over global function fields IV:S-unit equations in several variables with an application to norm form equations*, J. Number Theory (to appear).

[7] R.C. Mason, *Diophantine equations over function fields.*. London Mathematical Society Lecture Note Series, 96. Cambridge etc.: Cambridge University Press. X, 125 p., 1984.

[8] José Méndez Omaña and Michael E. Pohst, *Factoring polynomials over global fields. II.*, J. Symb. Comput. 40 (2005), pp. 1325–1339.

[9] M. Pohst and Hans Zassenhaus, *Algorithmic algebraic number theory.*. Encyclopedia of Mathematics and its Applications, 30. Cambridge etc.: Cambridge University Press. xiv, 465 p., 1989.

[10] Martin Schörnig, *Untersuchungen konstruktiver Probleme in globalen Funktionenkörpern*, Thesis, TU Berlin (1996).

[11] Denis Simon, *Solving norm equations in relative number fields using S-units.*, Math. Comput. 71 (2002), pp. 1287–1305.

Received 30 December, 2008; revised 1 October, 2009

Author information

István Gaál, University of Debrecen, Mathematical Institute
H-4010 Debrecen Pf. 12, Hungary.
Email: `igaal@math.klte.hu`

Michael E. Pohst, Technische Universtät Berlin, Institut für Mathematik MA 8-1
Straße des 17. Juni 136, 10623 Berlin, Germany.
Email: `pohst@math.tu-berlin.de`