*Functiones et Approximatio*
*XXXIX.1 (2008), 97–102*

# DIOPHANTINE EQUATIONS OVER GLOBAL FUNCTION FIELDS III: AN APPLICATION TO RESULTANT FORM EQUATIONS

István Gaál*, Michael Pohst

Dedicated to
Professor Władysław Narkiewicz
on his 70th birthday

**Abstract:** We give an efficient algorithm for solving resultant form equations over global function fields. This is the first time that such equations are reduced to unit equations in two variables and all solutions are determined.
**Keywords:** global function fields; unit equations; resultant form equations

## 1. Introduction

Let $f$ be a fixed polynomial over an integral domain $R$, let $0 \neq r \in R$ and consider those polynomials $g \in R[x]$ for which

$$\mathrm{Res}(f, g) = r. \tag{1.1}$$

Under various assumptions several authors considered the above resultant type equation mainly in the number field case, see e.g. W. M. Schmidt [12], J. H. Evertse and K. Győry [3]. For a fixed $f$ I. Gaál [5] gave an efficient algorithm to find all monic quadratic $g$ satisfying the equation. Polynomials of "small" height satisfying the equation were calculated by I. Járási [8].

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

In [6] and [7] we considered *function fields over finite fields* (without assuming the constant field to be algebraically closed). We developed an algorithm for solving unit equations in two variables and also Thue equations over such function fields.

**2000 Mathematics Subject Classification:** 11D57, 11Y50.
*Research supported in part by T042985 and T048791 from the Hungarian National Foundation for Scientific Research

Resultant type equations were until now usually reduced to unit equations in three variables. If $\alpha_1, \dots, \alpha_n \in R$ are the roots of $f$ and $\beta_1, \dots, \beta_m \in R$ are the roots of $g$, then the identity

$$(\alpha_i - \beta_k) - (\alpha_i - \beta_l) + (\alpha_j - \beta_l) - (\alpha_j - \beta_k) = 0$$

implies

$$\frac{\alpha_i - \beta_k}{\alpha_j - \beta_k} - \frac{\alpha_i - \beta_l}{\alpha_j - \beta_k} + \frac{\alpha_j - \beta_l}{\alpha_j - \beta_k} = 1,$$

where by equation (1.1) the fractions are elements of a suitable group of S-units of $R$. This approach did not enable one to derive effective results over number fields, since no effective theorems for unit equations in three variables exist.

In this paper we are going to solve completely resultant type equations over global function fields by reducing them to unit equations in two variables and applying the results of [6] and [7]. This is the first time that resultant form equations are solved completely.

## 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 $V_\infty$. For a non-zero element $f \in K$ we denote by $v(f)$ the value 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

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

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

$$\gamma_1 + \gamma_2 + \gamma_3 = 0 \ , \tag{2.1}$$

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

Since the next lemma will be applied frequently in this paper we excerpt it from [6] for the convenience of the reader.

**Lemma 2.1.** *Let $V_0$ be a finite subset of $V$ and let $\gamma_i$ $(1 \leq i \leq 3)$ be $V_0$-units satisfying (2.1). Then either $\frac{\gamma_1}{\gamma_3}$ is in $K^p$ or its height is bounded:*

$$H\left(\frac{\gamma_1}{\gamma_3}\right) \leq 2g - 2 + \sum_{v \in V_0} \deg v \ . \tag{2.2}$$

Note that equation (2.1) 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 $\gamma_1/\gamma_3$ and $\gamma_2/\gamma_3$ are $V_0$-units which makes the set $V_0$ smaller, cf. the proof of Lemma 3.1 in [6].

## 3. Solving resultant type equations over global function fields

Let us again use the notation of Section 2 about function fields. Assume that $f(x)$ is a monic polynomial of degree $n \geq 2$ with roots $\alpha_1, \ldots, \alpha_n$ contained in $O_K$. We assume that $f$ has at least two distinct roots, say $\alpha_1, \alpha_2$. Let $0 \neq r \in O_K$ and $m \in \mathbb{N}$ be given. Our purpose is to determine the monic polynomials $g(x)$ of degree $m$ with roots $\beta_1, \ldots, \beta_m \in O_K$ $(m \geq 2)$ satisfying

$$\mathrm{Res}(f, g) = r. \tag{3.1}$$

Recall that for the above polynomials

$$\mathrm{Res}(f, g) = \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

Note that if all roots of $g$ are equal to $\beta$ then equation (3.1) can be written in the form

$$(-1)^{mn}(f(\beta))^m = r.$$

That equation can be solved easily in the only unknown $\beta$.

Let $V_0$ denote the set of all valuations $v$ with $v(r) \neq 0$, assume that the infinite valuations are in $V_0$. By equation (3.1) any $\alpha_i - \beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ is a $V_0$–unit ($r \neq 0$ implies $\alpha_i \neq \beta_j$).

Observe that

$$\frac{\alpha_1 - \beta_i}{\alpha_1 - \alpha_2} + \frac{\beta_i - \alpha_2}{\alpha_1 - \alpha_2} = 1. \tag{3.2}$$

Let $V_1$ be the set of valuations containing $V_0$ and those valuations occurring in $\alpha_1 - \alpha_2$. Then both summands in (3.2) are $V_1$-units and Lemma 2.1 can be applied. Note that $p$-th powers can usually be excluded by considering the valuations in

$V_1 \backslash V_0$ for which the value of the numerator is zero and the value of the denominator is not divisible by $p$.

If no $p$-th powers can occur as solutions, Lemma 2.1 gives

$$H\left(\frac{\alpha_1-\beta_i}{\alpha_1-\alpha_2}\right) \le 2g-2+\sum_{v\in V_0}\deg v = c_1,$$

whence

$$H(\alpha_1-\beta_i) \le c_1 + H(\alpha_1-\alpha_2) = c_2.$$

Hence, we have to calculate all $V_0$-units $\alpha_1-\beta_i$ of height $\le c_2$. This can be done easily by using an idea of [7]. (It is much faster than calculating all $V_1$ units of height $\le c_1$.) For all possible values of $\alpha_1-\beta_i$ we test if

$$\beta_i-\alpha_2 = (\alpha_1-\alpha_2)\left(1-\frac{\alpha_1-\beta_i}{\alpha_1-\alpha_2}\right)$$

is also a $V_0$-unit. In this way we get the possible values of $\beta_i-\alpha_2$ from which the possible values of $\beta_i$ can be calculated and the polynomials $g$ that are possible solutions of (3.1) can be constructed.

## 4. Examples

We illustrate our method by two examples.

**Example 4.1.** Let $k=\mathbb{F}_5$ and let $\alpha$ be a root of

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

Let $K=k(t)(\alpha)$ and denote by $O_K$ the integral closure of $k[t]$ in $K$. This field is Galois, it is in fact $K=k(t)(\sqrt{t},\sqrt{t+1})$, a biquadratic field. The roots of $f$ are

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

We are going to determine all monic polynomials $g(x)$ of degree 4 with coefficients in $k[t]$ and with roots $\beta_1,\beta_2,\beta_3,\beta_4\in O_K$, satisfying

$$\mathrm{Res}(f,g) = c \tag{4.1}$$

with a non-zero $c\in k$. The field $K$ has genus 0 and there are two infinite valuations $v_{\infty,1}, v_{\infty,2}$, both of degree 1. We set $V_0=\{v_{\infty,1},v_{\infty,2}\}$. Then all $\alpha_i-\beta_j$ are $V_0$–units.

The element $\alpha_1-\alpha_2$ has two additional valuations $v_{t,1}, v_{t,2}$ corresponding to the polynomial $t$, both of degree 1. The element $\alpha_1-\alpha_2$ has value 1 at both of these valuations, hence $p$-th powers can be excluded. Let $V_1 = V_0 \cup \{v_{t,1}, v_{t,2}\}$. Then we obtain $c_2 = 4$. Searching over all possible $V_0$-units of height $\leq 4$ we obtain two possible elements $\beta_i$, namely $\beta_i = 0$ and $\beta_i = (4t+3)\alpha_1 + 4\alpha_1^3$. This second element is a quadratic element, giving rise to the polynomial $x^2 + (t+1)$. Testing $g(x) = (x^2 + (t+1))^2$, $g(x) = x^2(x^2 + (t+1))$ and $g(x) = x^4$ we find that the only solution is $g(x) = x^4$ with $\mathrm{Res}(f, g) = 1$.

**Example 4.2.** Let $k = \mathbb{F}_5$ and let $\alpha$ be a root of

$$z^5 - z - t = 0.$$

Let $K = k(t)(\alpha)$ and denote by $O_K$ the integral closure of $k[t]$ in $K$. This field is again Galois. If we denote by $\alpha_1$ a root of $f$, then the other four roots are

$$\alpha_i = \alpha_{i-1} + 1 \quad (i = 2, 3, 4, 5)$$

(Artin-Schreier extension).

We are going to determine all monic irreducible polynomials $g(x)$ of degree 5 with coefficients in $k[t]$ and with roots $\beta_i \in O_K$ $(i = 1, \ldots, 5)$, satisfying

$$\mathrm{Res}(f, g) = c \cdot t^5 \tag{4.2}$$

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

The field $K$ has genus 0, there is one infinite valuation $v_\infty$ of degree 1 and there are five valuations $v_{t,i}$ $(i = 1, \ldots, 5)$ corresponding to $t$, all of degree 1. We set $V_0 = \{v_\infty, v_{t,1}, v_{t,2}, v_{t,3}, v_{t,4}, v_{t,5}\}$. Then all $\alpha_i - \beta_j$ are $V_0$–units.

In this example we have $\alpha_1 - \alpha_2 = -1$ that is $V_1 = V_0$. We construct all $V_0$-units $\alpha_1 - \beta_i$ of height $\leq 4$ and test if

$$\beta_i - \alpha_2 = (-1) - (\alpha_1 - \beta_i)$$

is also a $V_0$-unit. There are 1145 such elements, and testing all possible values of $\beta_i$ (of degree 5 because $g$ is irreducible) we obtain only the solution $g(x) = x^5 + 4x + t$ of equation (4.2) for which

$$\mathrm{Res}(f, g) = 2\ t^5.$$

Consider now the solutions of equation (3.2) which are $p^h$-th powers of the other 1145 solutions of the unit equation. Then by $\alpha_1 - \alpha_2 = -1$ obviously also $\alpha_1 - \beta_i$ is a $p^h$-th power. Using conjugations the same holds for $\alpha_{1+j} - \beta_{i+j}$ $(j = 1, \ldots, 4)$, as well (the indices are to be calculated mod 5). Since $\alpha_i = \alpha_1 + (i-1) \quad (i = 2, \ldots, 5)$, by adding 1,2,3,4 (all are 5-th powers in $k$) we get the remaining six differences $\alpha_i - \beta_j$ from the above three differences, and we obtain, that all differences, as well as $\mathrm{Res}(f, g)$ must be complete $p^h$-th powers in $K$. But the right-hand side of the equation is $ct^5$, whence only $h = 1$ is possible. Testing 5th powers of all 1145 solutions of the unit equation we do not get any further solutions of equation (4.2).

**Remark.** The computation of the first example took just a few seconds, the second example took a few minutes. All computations were performed with Kash [1].

## 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, K. Győry, *Finiteness criteria for decomposable form equations*, Acta Arith. **50** (1988), 357–379.

[3] J. H. Evertse, K. Győry, *Lower bounds for resultants I*, Compos. Math. **88** (1993), 1–23.

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

[5] I. Gaál, *On the resolution of resultant type equations*, J. Symbolic Comput. **34** (2002), 137–144.

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

[7] I. Gaál, M. Pohst, *Diophantine equations over global function fields II: S-integral solutions of Thue equations*, Experimental Mathematics, **15** (2006), 1–6.

[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.

[12] W. M. Schmidt, *Inequalities for resultants and for decomposable forms*, in: Diophantine approximation and its applications, pp. 235–253, Academic Press, New York, 1973.

**Addresses:** István Gaál, University of Debrecen, Mathematical Institute, H–4010 Debrecen Pf.12., Hungary

Michael Pohst, Technische Universtät Berlin, Institut für Mathematik, Straße des 17. Juni 136, Berlin, 10623 Germany

**E-mail:** igaal@math.klte.hu, pohst@math.tu-berlin.de

**Received:** 25 April 2007; **revised:** 28 March 2008