International Journal of Pure and Applied Mathematics
Volume 53 No. 3 2009, 307-317

DIOPHANTINE EQUATIONS OVER GLOBAL FUNCTION FIELDS V: RESULTANT EQUATIONS IN TWO UNKNOWN POLYNOMIALS

István Gaál[1 §], Michael Pohst[2]

[1]Mathematical Institute
University of Debrecen
Debrecen Pf. 12., H-4010, HUNGARY
e-mail: igaal@math.klte.hu

[2]Institut für Mathematik
Technische Universität Berlin
136, Straße des 17. Juni, Berlin, GERMANY
e-mail: pohst@math.tu-berlin.de

Abstract: We give an efficient algorithm to solve resultant type equations in two unknown polynomials over global function fields. The method is based on the complete resolution of unit equations in three variables over function fields. This is the first time when such equations are completely solved.

AMS Subject Classification: 11D57, 11Y50
Key Words: global function fields, unit equations, resultant type equations

1. Introduction

Let R be an integral domain, $0 \neq r \in R$ and let

$$f(x) = a_m x^m + \ldots + a_1 x + a_0, \quad g(x) = b_n x^n + \ldots + b_1 x + b_0$$

be polynomials with coefficients in R. The *resultant* of the polynomials f and g is defined by the determinant

Received: April 20, 2009

[§]Correspondence author

$$\mathrm{Res}(f,g)=\left|\begin{array}{cccccc} a_m & \cdots & a_0 & & & \\ & a_m & \cdots & a_0 & & \\ & \ddots & & \ddots & & \\ & & a_m & \cdots & a_0 & \\ b_n & \cdots & b_0 & & & \\ & b_n & \cdots & b_0 & & \\ & \ddots & & \ddots & & \\ & & b_n & \cdots & b_0 & \end{array}\right|,$$

where the first n rows contain the coefficients of f and the last m rows contain the coefficients of g. If $\alpha_1,\dots,\alpha_m$ are the roots of f and $\beta_1,\dots,\beta_n$ are the roots of g then we have

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

On the other hand we may ask *which polynomials f,g have the property to have a prescribed resultant*. Let $0\neq r\in R$ be given. It is a classical problem in the theory of Diophantine equations and their applications to consider *resultant type equations* of the form

$$\mathrm{Res}(f,g)=r\quad(\text{in}\ \ f,g\in R[x])\,, \tag{1}$$

where the variables are the polynomials $f,g\in R[x]$. In some results one of the polynomials, say f, is given and we intend to determine g (one variable case). In other results both f and g are unknowns (two variables case).

This equation can be considered as a polynomial Diophantine equation in the coefficients of the unknown polynomial(s).

Note that by

$$\mathrm{Res}(f,f')\ =\ (-1)^{m(m-1)/2}\ a_m\ D(f)$$

the resultant type equation is a generalization of the *discriminant type equation*

$$D(f)=r\quad(\text{in}\ \ f\in R[x])\,,$$

where the main task is to determine polynomials f of given discriminant.

Resultant type equations have an extensive literature. It is a special type of *decomposable form equations*, see e.g. W.M. Schmidt [20], H.P. Schlickewei [19], K. Győry [12].

Several assertions on resultant type equations are proved under some further conditions on the unknown polynomial(s) (e.g. restriction on the degrees). For the one variable case see e.g. K. Győry [12], for the two variables case (and generalizations to binary forms) see e.g. K. Győry [13], [14], J.H. Evertse and

K. Győry [4], K. Győry [15], A. Bérczes, J.H. Evertse and K. Győry [1], [2].

Resultant type equations are typically reduced to *unit equations in three variables*. Using the above notation we have the identity

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

which 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) the ratios are elements of a suitable group of S-units of R. As it is well known, in the number field case there are no effective results for the solutions of unit equations in three variables, but there are explicit upper bounds for the number of their solutions. Hence, most of the above cited results on resultant type equations prove the finiteness of the number of solutions of equation (1) or give upper bounds for the number of solutions of that equation.

The complete resolution of equation (1) is therefore not feasible in full generality over number fields by using the present Diophantine tools.

For a fixed f we could only determine the quadratic polynomials g satisfying (1), see I. Gaál [5].

We have only recently shown, that for a fixed f, the resolution of equation (1) in g can be reduced to a unit equation in two variables, see I. Gaál and M. Pohst [10]. This enabled us to determine explicitely the solutions of (1) in the one variable case. We also gave a slight improvement for the number of solutions of (1) in the one variable case [11].

Since in the two variables case it is not feasible to explicitely solve equation (1) in the number field case, it is certainly of interest to present *an algorithm for solving the analogous equation over function fields*. This is the main object of our paper. Note that this is done by using our result [9] on determining explicitely the solutions of unit equations in several variables. Using these tools *we give here the first algorithm for solving completely resultant type equations in two unknown polynomials* over function fields.

R.C. Mason [16], [18] described solutions of unit equations in two variables and in several variables over function fields over algebraically closed constant fields. In a series of papers [6], [7], [8], [9] we considered *Diophantine equations over global function fields*, that is over finite extensions of $k(t)$, where k is a finite field. We described the solutions of unit equations in two variables [6], which enabled us to give an algorithm for solving resultant type equations in one unknown polynomial [8]. Moreover, in [9] we succeded to describe the solutions of unit equations in several variables, as well. This is the main tool in the present paper.

2. Auxiliary Results

2.1. Notation

In this section we summarize our notation and recall the auxiliary results needed to deal with resultant type equations properly.

In the following $k = \mathrm{F}_q$ denotes a finite field of $q = p^d$ elements. The rational function field of k is $k(t)$. K will be a finite extension of $k(t)$ of degree n 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 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 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

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

2.2. Unit Equations in Two Variables

To solve the resultant type equation we shall deal with a unit equation in three variables, which will be reduced to a unit equation in two variables. Therefore we include here the lemma on 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*. We consider the equation

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

where the γ_i are V_0-units for a suitable set V_0. This can be written as

$$\left(-\frac{\gamma_1}{\gamma_3}\right) + \left(-\frac{\gamma_2}{\gamma_3}\right) = 1 \tag{2}$$

which is a unit equation in two variables. Note that it suffices to assume that

γ_1/γ_3 and γ_2/γ_3 are V_0-units.

Lemma 1. *For all solutions of equation (2) either $\frac{\gamma_1}{\gamma_3}$ is in K^p or its height is bounded:*

$$H\left(\frac{\gamma_1}{\gamma_3}\right) \le 2g_0 - 2 + \sum_{v \in V_0} \deg v \ . \tag{3}$$

2.3. Unit Equations in Several Variables

Here we recall our general result [9] on unit equations in several variables.

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

$$\gamma_1 + \ldots + \gamma_n = 0 \tag{4}$$

is obviously equivalent with the unit equation

$$\left(-\frac{\gamma_1}{\gamma_n}\right) + \ldots + \left(-\frac{\gamma_{n-1}}{\gamma_n}\right) = 1 \tag{5}$$

in $n-1$ variables (note that it suffices if the fractions in (5) are V_0-units).

Lemma 2. *Assume that no proper subsum of the sum in (4) vanishes. Then we can explicitly construct a finite subset N of V, such that*

$$\frac{\gamma_1}{\gamma_n} = x_{1n} \cdot \Phi \ , \tag{6}$$

where x_{1n} is a solution of the $V_0 \cup N$-unit equation

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

and Φ is a $V_0 \cup N$-unit satisfying

$$H(\Phi) \le 2g_0 - 2 + \sum_{v \in V_0} \deg v \ . \tag{7}$$

3. Solving Resultant Type Equations in Two Unknown Polynomials

Assume that $f(x), g(x)$ are monic polynomials of degree $m, n \ge 2$, respectively. Assume that the (unknown) roots $\alpha_1, \dots, \alpha_m$ of f and $\beta_1, \dots, \beta_n$ of g are contained in O_K. Let $0 \ne r \in O_K$ and the degrees m, n be given and consider the solutions f, g of the equation

$$\mathrm{Res}(f, g) = r. \tag{8}$$

Under the above assumptions our algorithm makes possible to determine the roots of f, g. Note that this is a more general approach than usual. Our polynomials f, g having roots in O_K also have coefficients in O_K. If $r \in k[t]$ by considering the roots of f, g we can select those polynomials f, g that have coefficients in $k[t]$. Therefore our method covers the classical approach, as well.

Recall that for the above polynomials we have

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

If $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ satisfy this equation, then for any $\delta \in O_K$ $\alpha_1 + \delta, \ldots, \alpha_m + \delta$ and $\beta_1 + \delta, \ldots, \beta_n + \delta$ is also a set of solutions. Therefore obviously we can determine the roots only up to translation by elements of O_K.

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 (8) any $\alpha_i - \beta_j$ $(1 \leq i \leq m, 1 \leq j \leq n)$ is a V_0–unit ($r \neq 0$ implies $\alpha_i \neq \beta_j$).

To proceed systematically we use equations of type

$$\frac{\alpha_1 - \beta_j}{\alpha_1 - \beta_1} + \frac{\beta_j - \alpha_i}{\alpha_1 - \beta_1} + \frac{\alpha_i - \beta_1}{\alpha_1 - \beta_1} = 1, \tag{9}$$

where all fractions are V_0-units. By Lemma 2 we can represent the above fractions in the form

$$\frac{\alpha_1 - \beta_j}{\alpha_1 - \beta_1} = -x_0\Phi, \quad \frac{\beta_j - \alpha_i}{\alpha_1 - \beta_1} = -y_0\Psi, \quad \frac{\alpha_i - \beta_1}{\alpha_1 - \beta_1} = -z_0\Lambda, \tag{10}$$

where x_0, y_0, z_0 are solutions of $V_0 \cup N$-unit equations in two variables of type $x + y = 1$, and Φ, Ψ, Λ are $V_0 \cup N$-units of bounded heights. Here the valuation set N (usually containing just a few elements) can be explicitely determined. There are a finite number of possible values of Φ, Ψ, Λ. By Lemma 1 we can calculate a finite number of possible elements such that x_0, y_0, z_0 either belong to that set, or equal p^κ-th powers of elements of that set.

It follows from the arguments of [9] that two of x_0, y_0, z_0, say x_0, y_0 are corresponding solutions of the unit equation in two variables, that is $x_0 + y_0 = 1$. This implies that x_0 is a p^κ-th power if and only if y_0 is one. The above representation implies

$$x_0\Phi + y_0\Psi + z_0\Lambda = -1. \tag{11}$$

In Section 5 of [9] we described a simple method to exclude p^κ-th powers. If all of x_0, y_0, z_0 are p^κ-th powers, then by $y_0 = 1 - x_0$ we get

$$x_0(\Phi - \Psi) + z_0\Lambda = -1 - \Psi. \tag{12}$$

Using local derivation at a valuation we obtain
$$x_0(\Phi' - \Psi') + z_0\Lambda' = -\Psi'. \tag{13}$$
For given values of Φ, Ψ, Λ this system of equations usually determines x_0, z_0 and y_0 can be calculated from equation (11). Else we apply higher derivatives.

If some of x_0, y_0, z_0, say x_0 is not a p^κ-th power, then the corresponding $y_0 = 1 - x_0$ is also not p^κ-th power. Then the finitely many possibilities for x_0, y_0, and z_0 can be calculated from equation (11).

This way we calculate (the possible values of)
$$\eta_{ij} = \frac{\alpha_i - \beta_j}{\alpha_1 - \beta_1}.$$
In order to determine $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ we need this value for all i, j. Note that for this purpose we usually do not need to solve mn unit equations in three variables. Combining the three fractions in (9) and using Galois automorphisms we often can calculate several further fractions of this type (cf. also our example).

Finally, by
$$(\alpha_1 - \beta_1)^{mn} \; = \; r \cdot \prod_{i=1}^{m} \prod_{j=1}^{n} \eta_{ij}^{-1} \tag{14}$$
we may calculate $\alpha_1 - \beta_1$, and using η_{ij} the values of $\alpha_i - \beta_j$, as well. These enable us to derive
$$\beta_i - \beta_j = (\alpha_k - \beta_j) - (\alpha_k - \beta_i).$$
Now fixing, say β_1, in O_K we obtain $\beta_2, \ldots, \beta_n$ as well as $\alpha_1, \ldots, \alpha_m$.

4. Example

We illustrate our method by the following example.

Let $k = \mathrm{F}_3$ and let $\xi = \xi_1$ be a root of
$$p(z) = z^3 - tz^2 - (t+3)z - 1 = 0.$$
Let $K = k(t)(\xi)$ and denote by O_K the integral closure of $k[t]$ in K. The field K has genus $g_0 = 0$. This field is Galois (the well known family of simplest cubic fields), its cyclic Galois group is generated by σ. Setting $\xi_1 = \xi$ we get
$$\xi_2 = \sigma(\xi_1) = \frac{-1}{\xi_1 + 1}, \quad \xi_3 = \sigma(\xi_2) = \frac{-1}{\xi_2 + 1}.$$

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

$$\mathrm{Res}(f,g) = r \tag{15}$$

in cubic polynomials f, g with roots in O_K. We are going to solve the unit equation

$$\frac{\alpha_1-\beta_2}{\alpha_1-\beta_1}+\frac{\beta_2-\alpha_2}{\alpha_1-\beta_1}+\frac{\alpha_2-\beta_1}{\alpha_1-\beta_1}=1.$$

The set V_0 consists of the three infinite valuations v_1, v_2, v_3 of K, each of degree 1. For the set of new valuations N we have (see [9])

$$\sum_{v\in N}\deg v \le 2g_0 - 2 + \sum_{v\in V_0}\deg v = 1.$$

Factoring $t^3 - t$ over k we find that the only valuation satisfying this condition is v_t, the valuation correspontong to t, having degree 1: $N = \{v_t\}$.

In case there are 3^κ-th powers among x_0, y_0, z_0 in equation (11), then by $2g_0 - 2 + \sum_{v\in V_0}\deg v < p = 3$ these elements are in fact V_0-units, as well as Φ, Ψ, Λ (see Remark 3 after the main theorem in [9]). Up to constant factors there are 7 V_0-units of height ≤ 1 in K. Considering all possible values of Φ, Ψ, Λ and solving the system of equations (12), (13) we could always show, that the x_0, y_0, z_0 are at most 3^1-st powers of appropriate V_0 units. These values will be considered together with all other possible values of x_0, y_0, z_0 in the following.

In case x_0, y_0, z_0 are not 3^κ-th powers, then Φ, Ψ, Λ are indeed $V_0 \cup N$-units of height ≤ 1. There are 13 such elements (up to constant factors). Moreover, x_0, y_0, z_0 are solutions of $x + y = 1$ in $V_0 \cup N$-units. There are 61 solutions of this equation (which are no 3-rd powers). It suffices to consider all possible values of Φ, Ψ and x_0, since $y_0 = 1 - x_0$ and $z_0\Lambda = -1 - x_0\Phi - (1 - x_0)\Psi$. This yields $61 \cdot 26^2 = 41236$ cases to test. To include the possible 3-rd powers discussed in the preceeding section we also tested x_0^3 in the role of x_0.

The elements

$$\eta_{ij} = \frac{\alpha_i - \beta_j}{\alpha_1 - \beta_1}\,,$$

were calculated in the following way (cf. (10):

$$\begin{aligned}
\eta_{11} &= 1\,,\\
\eta_{12} &= -x_0\Phi\,,\\
\eta_{22} &= (1-x_0)\Psi\,,\\
\eta_{33} &= (\sigma^2(\eta_{22}))^{-1}\,,\\
\eta_{21} &= 1 + x_0\Phi + (1-x_0)\Psi\,,\\
\eta_{13} &= \eta_{33}\cdot\sigma^2(\eta_{21})\,,
\end{aligned}$$

$$\begin{aligned}\eta_{23} &= \eta_{21} - \eta_{11} + \eta_{13}\,,\\ \eta_{31} &= \eta_{33} - \eta_{23} + \eta_{21}\,,\\ \eta_{32} &= \eta_{31} - \eta_{21} + \eta_{22}\,.\end{aligned}$$

From these we calculated $\alpha_1 - \beta_1$ by (14), and then all $\alpha_i - \beta_j$. Thus we obtained all $\beta_i - \beta_j$ and finally all β_j and α_i.

In all solutions obtained one of the polynomials, say f, has three equal constant roots (in k). Therefore we fixed this constant to be zero and then $f(x) = x^3$ is the first term in all solutions (f, g) of equation (15).

In the following solutions $g(x)$ has constant roots:

$$g(x) = x^3 + 2,\;\; x^3 + 2x^2 + 2x + 1,\;\; x^3 + x^2 + 2x + 2,\;\; x^3 + 1.$$

In the next solutions $g(x)$ has coefficients in $k[t]$:

$$g(x) = x^3+tx^2+tx+2,\;\; x^3+tx^2+2tx+1,\;\; x^3+2tx^2+tx+1,\;\; x^3+2tx^2+2tx+2.$$

Moreover, there are a couple of solutions, where the coefficients of $g(x)$ are elements of $O_K \setminus k[t]$, i.e. $g(x) = x^3 + \gamma_2 x^2 + \gamma_1 x + \gamma_0$, where the coefficients of $\gamma_2, \gamma_1, \gamma_0$ in the basis $\{1, \xi, \xi^2\}$ of O_K are the following:

$$\begin{aligned}\gamma_2, \gamma_1, \gamma_0 = \quad & [2t+2, t+1, 2], [t+1, 1, 0], [1, 0, 0]\\ & [t, 1, 0], [2t, t, 2], [2, 0, 0]\\ & [t, 2t, 1], [2t, 2, 0], [2, 0, 0]\\ & [t+1, 1, 0], [2t+2, t+1, 2], [1, 0, 0]\\ & [t+1, 2t, 1], [t+2, 2t+2, 1], [1, 0, 0]\\ & [t+1, 2t+2, 1], [t+1, 1, 0], [2, 0, 0]\\ & [t+2, 2t+2, 1], [t+1, 2t, 1], [1, 0, 0]\\ & [2t, 2, 0], [2t, t, 2], [1, 0, 0]\\ & [2t, t, 2], [2t, 2, 0], [1, 0, 0]\\ & [2t+1, t+1, 2], [t+1, 2t, 1], [2, 0, 0]\\ & [2t+2, 2, 0], [2t+2, t+1, 2], [2, 0, 0]\\ & [2t+2, t, 2], [t+2, 2t+2, 1], [2, 0, 0]\,.\end{aligned}$$

Remark. The computation of the example took a couple of minutes. All computations were performed with Kant [3].

Acknowledgements

Research supported in part by K67580 and K75566 from the Hungarian National Foundation for Scientific Research.

References

[1] A. Bérczes, J.H. Evertse, K. Győry, Diophantine problems related to discriminants and resultants of binary forms, In: *Diophantine Geometry* (Ed. U. Zannier), Proc. Conf. Pisa, Italy, April 12-July 22, 2005. Pisa: Edizioni della Normale. Centro di Ricerca Matematica Ennio De Giorgi (CRM) Series (Nuova Serie) **4** (2007), 45-63.

[2] A. Bérczes, J.H. Evertse, K. Győry, On the number of pairs of binary forms with given degree and given resultant, *Acta Arith.*, **128** (2007), 19-54.

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

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

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

[8] I. Gaál, M. Pohst, Diophantine equations over global function fields III: An application to resultant form equations, *Functiones at Approximatio*, **XXXIX.1** (2008), 97-102.

[9] I. Gaál, M. Pohst, 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.

[10] I. Gaál, M. Pohst, Solving resultant form equations over number fields, *Math Comput.*, **77** (2008), 2447-2453.

[11] I. Gaál, M. Pohst, A note on the number of solutions of resultant equations, *JP Journal of Algebra, Number Theory and Applications*, **12** (2008), 185-189.

[12] K. Győry, Some applications of decomposable form equations to resultant equations, *Colloq. Math.*, **65** (1993), 267-275.

[13] K. Győry, On the number of pairs of polynomials with given resultant or given semi- resultant, *Acta Sci. Math.*, **57** (1993), 515-529.

[14] K. Győry, Some new results connected with resultants of polynomials and binary forms, *Grazer Math. Ber.*, **318** (1993), 17-27.

[15] K. Győry, Applications of unit equations, *RIMS Kokyuroku*, **958** (1996), 62-78.

[16] R.C. Mason, *Diophantine Equations over Function Fields*, Cambridge University Press, 1984.

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

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

[19] H.P. Schlickewei, Inequalities for decomposable forms, *Astrisque*, **41-42** (1977), 267-271.

[20] W.M. Schmidt, Inequalities for resultants and for decomposable forms, In: *Diophantine Approximation and its Applications*, 235-253, Academic Press, New York, 1973.