ACTA ARITHMETICA
XCIX.1 (2001)

Equations in one variable over function fields

by

Enrico Bombieri (Princeton, NJ), Julia Mueller (Bronx, NY)
and Umberto Zannier (Venezia)

1. Introduction. Let $K = k(t)$ be the field of rational functions of one variable over an algebraically closed field k of characteristic 0. In this paper we consider the following two types of equations. Let $a_1, \dots, a_n$ be non-zero elements of K, then the first type is

$$a_1 x^{p_1} + \dots + a_n x^{p_n} = 1 \tag{1.1}$$

where $n \geq 2$ and $p_1 > \dots > p_n \geq 1$ are fixed integers, while the second type deals with zeros of *exponential polynomials*:

$$a_1(m)\alpha_1^m + \dots + a_n(m)\alpha_n^m = 0 \tag{1.2}$$

where the *characteristic roots* $\alpha_i \in K^*$ are distinct and the polynomials $a_i(z) \in K[z]$ are not identically zero, to be solved for $m \in \mathbb{Z}$. Any linear recurrence determines an exponential polynomial, and equation (1.2) corresponds to studying the zeros of a linear recurrence in the function field K.

We are interested in the number of solutions of these two equations. There is an extensive literature on this problem and our aim here is that of giving a simple elementary approach to the question, based on the *abc*-theorem in function fields for equation (1.1) and the use of derivations for equation (1.2). The main feature of our bounds is their smallness and uniformity with respect to coefficients and exponents.

Definition. Let $x, x' \in K^*$. We say that x and x' are *proportional* if $x'/x \in k^*$.

Theorem 1. *The number of non-proportional solutions in K^* of equation* (1.1) *is at most n, provided* (1.1) *satisfies the following lacunarity condition*:

$$p_i - p_{i+1} > \lambda, \qquad i = 1, \dots, n, \tag{1.3}$$

2000 *Mathematics Subject Classification*: 11D61, 11Jxx.
Research of U. Zannier supported by a grant to the Institute for Advanced Study by the James D. Wolfensohn Fund.

where $p_{n+1} = 0$ *and*

$$\lambda = \tfrac{1}{2}(n+1)!((n+1)!-1)((n+1)!-2). \tag{1.4}$$

Remarks. The bound in Theorem 1 is sharp, because given n generic elements $x_1, \dots, x_n \in K^*$ we can solve (1.1) for $x = x_i$, $i = 1, \dots, n$, as a linear system of n equations in the n unknowns a_i. The non-proportionality of solutions is also needed, as one sees by taking all exponents p_i divisible by some integer N, because if x is a solution then εx is also a solution whenever ε is an Nth root of unity. Finally, some condition such as (1.3) is also needed. For example, the equation

$$-\frac{1}{(2t)^2(1-t^4)^2}\,x^6 + \frac{1+14t^4+t^8}{(2t)^2(1-t^4)^2}\,x^2 = 1$$

has the six solutions $x = \pm 2t$, $\pm(1-t^2)$, $\pm\sqrt{-1}(1+t^2)$ and in particular has three non-proportional solutions.

Our second theorem deals with recurrent sequences in function fields.

Theorem 2. *Let* $a_1, \dots, a_n \in K[x]$ *be non-zero polynomials of degree* $d_1, \dots, d_n$ *and suppose that* $\alpha_1, \dots, \alpha_n$ *are pairwise non-proportional. Then the number of integer solutions* m *of equation* (1.2) *is at most*

$$d_1 + \ldots + d_n + n(n-1)/2.$$

The method of proof of Theorem 2 works in a more general setting, in which the condition of non-proportionality is dropped. We can describe this as follows.

Let $I \subseteq \{1, \dots, n\}$ be a maximal subset of indices such that the elements α_i, $i \in I$, are pairwise non-proportional. Then every α_j is proportional to some α_i with $i \in I$ and equation (1.2) can be rewritten as

$$\sum_{i \in I} b_i(m)\alpha_i^m = 0, \tag{1.5}$$

where now the coefficients $b_i(z)$ are exponential polynomials with characteristic roots in k^* and coefficients in $K[z]$.

Definition. A solution m of (1.2) is called *isotrivial* if every $b_i(m) = 0$ in the decomposition (1.5).

Isotrivial solutions are precisely those solutions for which no information can be extracted by differentiation with respect to t. Let V be the k-vector space generated by the coefficients of the polynomials $a_i(z)$, $i = 0, \dots, n$. Then we can express the exponential polynomials $b_i(z)$ as linear combinations of a basis v_j of V, with coefficients suitable exponential polynomials $B_{ij}(z)$ defined over k and with characteristic roots in k^*. Since for $m \in \mathbb{Z}$ we have $B_{ij}(m) \in k$ and since the elements v_j are linearly independent over

k, the system of equations $b_i(m) = 0$, $i \in I$, is equivalent to the system $B_{ij}(m) = 0$, on which differentiation with respect to t acts trivially.

THEOREM 3. *Let $a_1, \ldots, a_n \in K[x]$ be non-zero polynomials of degree $d_1, \ldots, d_n$. Then the number of non-isotrivial integer solutions m of equation* (1.2) *is at most*

$$d_1 + \ldots + d_n + n(n-1)/2.$$

If $n = 3$ and the polynomials a_i are constants, Theorem 2 states that we have at most three solutions to equation (1.2), which is sharp. In fact, by making a translation we may suppose that $m = 0$ is the smallest solution. Now suppose $m = 0, 1$ are solutions and a_1, a_2, a_3 are constants in K. We may assume $\alpha_3 = 1$ and write $x = \alpha_1$, $y = \alpha_2$. Then equation (1.2) becomes

$$(1-y)x^m + (x-1)y^m - (x-y) = 0. \tag{1.6}$$

If $m = 3$ the left-hand side of (1.6) factorizes as $-(1-x)(1-y)(x-y)(1+x+y)$; therefore, if $K \cong k(t)$ is the function field of genus 0 given by the field of fractions of the ring $k[x,y]/(1+x+y)$, we obtain an example of (1.2) with three solutions $m = 0, 1, 3$ (note that $\alpha_1 = t$, $\alpha_2 = -1 - t$ and $\alpha_3 = 1$ are non-proportional). Another example is obtained by taking $m = 4$, where now the function field $K \cong k(t)$ of genus 0 is the field of fractions of the ring $k[x,y]/(1+x+y+x^2+xy+y^2)$ (in this last case, the isomorphism $K \cong k(t)$ requires that the associated conic contains a point rational over k).

Conversely, if (1.2) has three solutions $(0, l, m)$ in $k(t)$ then, after a change of variable $(x', y') = (x^{\pm a}, y^{\pm a})$ with $a = \mathrm{GCD}(l, m)$, equation (1.2) can be reduced to these two examples. We sketch the argument. Suppose 0, l, m with $1 \le l < m$ are three solutions with $\mathrm{GCD}(l, m) = 1$ and $m \ge 3$. Then in place of (1.6) we have the equation

$$(1-y^l)x^m + (x^l-1)y^m - (x^l - y^l) = 0. \tag{1.6$'$}$$

The plane curve defined by (1.6)$'$ consists of the three lines $x = 1$, $y = 1$, $x = y$ and the curve $C_{l,m}$ with equation

$$\frac{R(x) - R(y)}{x - y} = 0$$

with $R(x) = (x^m - 1)/(x^l - 1)$. One shows that $C_{l,m}$ is an absolutely irreducible curve, by proving that the equation $R(x) = w$ over $k(w)$ has Galois group the symmetric group S_{m-1}, and using the fact that S_{m-1} is doubly transitive. Once this is done, one computes the genus g of $C_{l,m}$ using Hurwitz's formula, obtaining $g = (m-3)(m-4)/2 + (l-1)(m-l-1)$. Hence $g = 0$ only if $m = 3$ or $m = 4$ and l is 1 or $m - 1$, proving what we want.

By contrast, the number of solutions of (1.2) in a number field can be higher and J. Berstel in 1974 produced an example with $n = 3$ and entries in a sextic field with 6 solutions (see F. Beukers [Be]). This corresponds to

the ternary recurrence

$$u_{m+3} = 2u_{m+2} - 4u_{m+1} + 4u_m, \qquad u_0 = u_1 = 0,\ u_2 = 1$$

where $u_m = 0$ for $m = 0, 1, 4, 6, 13, 52$. It is shown in [Be] that 6 is the maximum number of zeros of a ternary recurrence over $\mathbb{Z}$.

It is an interesting open problem to determine the precise upper bound for the number of solutions of (1.2) if $n > 3$, already in the case $d_1 = \ldots = d_n = 0$. The upper bound given by Theorem 2 is then $n(n-1)/2$, while the easy lower bound is n. The argument given above extends to general n as follows. Consider again the case in which every a_i is a constant in K and suppose that $m = 0, 1, \ldots, n-2$ are solutions. If we assume that there is another solution $n - 1 + p$ with $p \geq 0$ then the corresponding determinant $\det(\alpha_i^m)$ for $m = 0, \ldots, n-2, n-1+p$ must vanish. After division by the Vandermonde determinant with $m = 0, \ldots, n-2, n-1$ we obtain the complete s-function given by the sum of all monomials in $\alpha_1, \ldots, \alpha_n$ of degree p. In general, imposing the vanishing for an arbitrary set of exponents leads to the study of general Schur s-functions. In this way, one finds rather easily infinitely many examples of equation (1.2) with $2n-2$ solutions with algebraic characteristic roots α_i and with $2n-3$ solutions with α_i in an algebraic function field in one variable. To see this, note that imposing the vanishing for $p = 1, \ldots, n-2$ is equivalent to setting to 0 the first $n-2$ elementary s-functions of $\alpha_1, \ldots, \alpha_n$. Hence the associated complete intersection is the locus in $\mathbb{P}^{n-1}$ of $(\alpha_1, \ldots, \alpha_n)$ where α_i, $i = 1, \ldots, n$, run over a complete ordered set of roots of the equation

$$\alpha^n + u\alpha + v = 0$$

with $v \neq 0$. This locus is an irreducible curve C_n of genus $n!/4 - (n-1)! - (n-2)!/2 + 1$ (setting $v = 1$ leads to the cyclic covering $\widetilde{C}_n \to C_n$ given by $(\alpha_1, \ldots, \alpha_n, u) \mapsto (\alpha_1, \ldots, \alpha_n)$ with group action

$$(\alpha_1, \ldots, \alpha_n, u) \mapsto (\varepsilon\alpha_1, \ldots, \varepsilon\alpha_n, \varepsilon^{-1}u)$$

with $\varepsilon^n = 1$; now apply Hurwitz's genus formula to get first the genus of $\widetilde{C}_n$, then the genus of C_n).

For $n = 4$, taking $m = 0, 1, 2, 4, 5$ leads to a function field of genus 0 and to an equation (1.2) in 4 variables defined over $k(t)$, with 5 solutions; the upper bound given by Theorem 2 is 6 solutions. For larger n, the question amounts to finding rational curves in these complete intersections and general arguments can be used to show that the number of solutions of an equation (1.2) over $k(t)$ can be as large as $n + c(n)$, where $c(n)$ tends rather slowly to infinity with n.

Finally, in the last section of this paper we indicate some variants of Theorem 3 which may be of independent interest.

We should mention here the important paper [SSW] of H. P. Schlickewei, W. M. Schmidt and M. Waldschmidt, culminating in Schmidt's paper [Schm] proving a uniform bound depending only on n for the number solutions of (1.2) if K is a number field, provided α_i/α_j is not a root of unity for $i \neq j$. The proofs of these results depend on deep versions of Schmidt's celebrated Subspace Theorem, as well as on delicate combinatorial and number theoretic arguments. Specialization arguments can be used to deduce bounds for the number of solutions of equation (1.2) over a function field from the bounds given in these papers for the more difficult algebraic case, but it appears that our method of counting non-isotrivial solutions yields sharper results.

Finally, the results and methods of this paper extend quite easily to base function fields of transcendence degree 1 and positive genus.

2. Auxiliary results. We denote by M_K the set of all places of K and for $v \in M_K$ we associate an additive valuation $v(\ )$ normalized so that the sum formula

$$\sum_{v \in M_K} v(x) = 0$$

holds for $x \in K^*$.

Assume that equation (1.1) has $n+1$ non-proportional solutions. For a fixed $v \in M_K$ we order our set of solutions x_i, $i = 1, \ldots, n+1$, so that

$$v(x_1) \geq \ldots \geq v(x_{n+1}). \tag{2.1}$$

Now we apply a familiar argument whose purpose is to obtain a relation among the solutions x_i which is independent of the coefficients a_i of (1.1). In the language of the paper [CHM] by L. Caporaso, J. Harris and B. Mazur, this amounts to finding an explicit *correlation* among the solutions x_i, $i = 1, \ldots, n+1$. If we view (1.1), evaluated at $x = x_i$, as a linear relation among the coefficients a_i and the constant 1, we see that

$$\det \begin{pmatrix} x_1^{p_1} & x_1^{p_2} & \ldots & x_1^{p_{n+1}} \\ x_2^{p_1} & x_2^{p_2} & \ldots & x_2^{p_{n+1}} \\ \vdots & \vdots & \ldots & \vdots \\ x_{n+1}^{p_1} & x_{n+1}^{p_2} & \ldots & x_{n+1}^{p_{n+1}} \end{pmatrix} = \sum_{\sigma \in \mathcal{S}} m_\sigma = 0, \tag{2.2}$$

where $p_1 > \ldots > p_n > p_{n+1} = 0$, where $\mathcal{S}$ is the set of permutations of $\{1, \ldots, n+1\}$ and where we have abbreviated

$$m_\sigma = \varepsilon(\sigma) x_{\sigma(1)}^{p_1} x_{\sigma(2)}^{p_2} \cdots x_{\sigma(n+1)}^{p_{n+1}}$$

with $\varepsilon(\sigma) = \pm 1$ the parity of the permutation σ.

Let $I = \{1, \dots, n+1\}$, let q_k, $k = 1, \dots, l$, be the distinct values of $v(x_i)$ arranged in decreasing order and define

$$I_k = \{i \in I \,:\, v(x_i) = q_k\}, \qquad t_k = |I_k|.$$

Then

$$I = \bigcup_{k=1}^{l} I_k, \qquad \sum_{k=1}^{l} t_k = n+1. \tag{2.3}$$

Let $\mathcal{S}_0$ be the subset of permutations given by

$$\mathcal{S}_0 = \{\sigma \in S : \sigma(I_k) = I_k,\ 1 \le k \le l\}.$$

We have

LEMMA 1. *Let* $M = \max v(m_\sigma)$. *Then*

$$\mathcal{S}_0 = \{\sigma \in \mathcal{S} : v(m_\sigma) = M\}. \tag{2.4}$$

Moreover, if $\sigma \notin \mathcal{S}_0$ *we have*

$$v(m_\sigma) < M - \lambda \tag{2.5}$$

with $\lambda = \frac{1}{2}(n+1)!((n+1)! - 1)((n+1)! - 2)$.

Proof. Suppose $\sigma \in \mathcal{S}_0$. Then for $i \in I_k$ we have $v(x_{\sigma(i)}) = v(x_i)$ and $v(m_\sigma) = v(m_{id}) = M$, because

$$v(m_{id}) = \sum_{i=1}^{n+1} p_i v(x_i)$$

and because the integers p_i and $v(x_i)$ form decreasing sequences. This proves that

$$\mathcal{S}_0 \subseteq \{\sigma \in \mathcal{S} : v(m_\sigma) = M\}.$$

The inclusion in the other direction is proven as follows. Suppose $\sigma \notin \mathcal{S}_0$. Then we claim that there is a pair (i, j) with $i < j$ and $\sigma(i) \in I_{k_1}$, $\sigma(j) \in I_{k_2}$ but $k_1 > k_2$. Indeed if this were not the case then whenever $i < j$ we would have $\sigma(i) \in I_{k_1}$, $\sigma(j) \in I_{k_2}$ and $k_1 \le k_2$. Since $\sigma \notin \mathcal{S}_0$, there would be a first element i with $i \in I_{k_0}$ but $\sigma(i) \notin I_{k_0}$. Note that since i is the first such element we must have $\sigma(I_1) = I_1$, ..., $\sigma(I_{k_0-1}) = I_{k_0-1}$. Hence $i \in I_{k_1}$ and $k_1 > k_0$. Now our assumption was that if $i < j$ and $i \in I_{k_1}$ then $j \in I_{k_2}$ with $k_2 \ge k_1$; therefore,

$$\sigma(\{i, i+1, \dots, n+1\}) \subseteq \bigcup_{k=k_1}^{l} I_k. \tag{2.6}$$

On the other hand, the union on the right-hand side of (2.6) is a proper subset of $\{i, i+1, \dots, n+1\}$ because $i \in I_{k_0}$ and $k_0 < k_1$. This contradicts the fact that σ is a permutation and proves our claim.

Now let (i,j) be as in our claim and define a new permutation τ by $\tau(i)=\sigma(j)$, $\tau(j)=\sigma(i)$, and $\tau(k)=\sigma(k)$ for $k\neq i,j$. Then $v(x_{\sigma(j)})>v(x_{\sigma(i)})$ because $k_2<k_1$ and we have

$$\begin{aligned} v(m_\tau)-v(m_\sigma) &= p_i v(x_{\sigma(j)})+p_j v(x_{\sigma(i)})-p_i v(x_{\sigma(i)})-p_j v(x_{\sigma(j)}) \\ &= (p_i-p_j)(v(x_{\sigma(j)})-v(x_{\sigma(i)}))\geq p_i-p_j>\lambda. \end{aligned}$$

This proves both (2.4) and (2.5) and completes the proof of Lemma 1.

We abbreviate $T_k=t_1+\ldots+t_k$ and

$$D_k=\det\begin{pmatrix} x_{T_{k-1}+1}^{p_{T_{k-1}+1}} & x_{T_{k-1}+1}^{p_{T_{k-1}+2}} & \ldots & x_{T_{k-1}+1}^{p_{T_k}} \\ \vdots & \vdots & \ldots & \vdots \\ x_{T_k}^{p_{T_{k-1}+1}} & x_{T_k}^{p_{T_{k-1}+2}} & \ldots & x_{T_k}^{p_{T_k}} \end{pmatrix}.$$

We have

Lemma 2.

$$\prod_{k=1}^{l} D_k=\sum_{\sigma\in\mathcal{S}_0} m_\sigma.$$

Proof. Clear by multiplying the Laplace expansions of the determinants.

3. Proof of Theorem 1. We prove Theorem 1 by induction on n, using a determinantal technique already introduced in the papers [BoM1] and [BoM2]. If $n=1$, the result is obvious. Hence suppose $n\geq 2$ and that the theorem has been verified for equations with less than $n+1$ monomials. Our first objective is to show that if $v(x_i)$ is not constant for $i=1,\ldots,n+1$ then

$$\sum_{\sigma\in\mathcal{S}_0} m_\sigma\neq 0. \tag{3.1}$$

Suppose this is not the case. Then Lemma 2 shows that some $D_k=0$. Thus we can find a non-zero solution $(b_1,\ldots,b_{t_k})$ to

$$\begin{pmatrix} x_{T_{k-1}+1}^{p_{T_{k-1}+1}} & x_{T_{k-1}+1}^{p_{T_{k-1}+2}} & \ldots & x_{T_{k-1}+1}^{p_{T_k}} \\ \vdots & \vdots & \ldots & \vdots \\ x_{T_k}^{p_{T_{k-1}+1}} & x_{T_k}^{p_{T_{k-1}+2}} & \ldots & x_{T_k}^{p_{T_k}} \end{pmatrix}\cdot\begin{pmatrix} b_1 \\ \vdots \\ b_{t_k} \end{pmatrix}=0.$$

This means that the equation

$$b_1 x^{p_{T_{k-1}+1}}+\ldots+b_{t_k}x^{p_{T_k}}=0 \tag{3.2}$$

has at least t_k distinct solutions, namely x_i for $i=T_{k-1}+1,\ldots,T_k$. Now we note that the gap condition (1.3) remains valid for the exponents in (3.2), and we also remark that the decomposition $I=\bigcup_{k=1}^{l} I_k$ has $l\geq 2$, because $v(x_i)$ is not constant for $i=1,\ldots,n+1$ by hypothesis. It follows that

$t_k \le n$. Now equation (3.2) is readily reduced to an equation of type (1.1) but with a strictly smaller number $m+1$ of monomials, and with at least $t_k \ge m+1$ distinct solutions. This contradicts the induction hypothesis and proves (3.1).

Our next tool is the *abc*-inequality in function fields [BrM], [V], which we state in the following form:

Let $u_i \in K^*$, $i = 1, \dots, m$, be such that $\sum u_i = 0$ and no proper subsum of this sum vanishes. Then

$$-\sum_v \min v(u_i) \le \frac{(m-1)(m-2)}{2}\,|S|$$

where $\sum_v$ runs over all places of K and where S is the set of places v for which $v(u_i) \ne 0$ for some i.

The product formula $\sum_v v(u_j) = 0$ yields

$$\sum_v (v(u_j) - \min v(u_i)) \le \frac{(m-1)(m-2)}{2}\,|S|$$

whence, summing over j, we infer

$$\sum_v (\max v(u_j) - \min v(u_i)) \le \frac{1}{2} m(m-1)(m-2) \cdot |\{v : \max_i v(u_i) - \min_j v(u_j) > 0\}|. \tag{3.3}$$

For the purpose of applying (3.3) we fix a decomposition of (2.2) into vanishing subsums

$$\sum_{\sigma \in \mathcal{S}} m_\sigma = \sum_{\mathcal{B}} \sum_{\sigma \in \mathcal{B}} m_\sigma$$

where

$$\sum_{\sigma \in \mathcal{B}} m_\sigma = 0 \tag{3.4}$$

for each $\mathcal{B}$, while no proper subsum of (3.4) vanishes. We call $\mathcal{B}$ a *component* of $\mathcal{S}$ and refer to $\mathcal{B}$ as an *irreducible block*. For a given v and $\mathcal{B}$, we write

$$I_v(\mathcal{B}) = \max_{\sigma \in \mathcal{B}} v(m_\sigma) - \min_{\sigma \in \mathcal{B}} v(m_\sigma).$$

We apply (3.3) to each sum (3.4) and get

$$\sum_{\mathcal{B}} \sum_v I_v(\mathcal{B}) \le \sum_{\mathcal{B}} \frac{1}{2} |\mathcal{B}|(|\mathcal{B}|-1)(|\mathcal{B}|-2) \cdot |\{v : I_v(\mathcal{B}) > 0\}| \le \lambda \cdot |S| \tag{3.5}$$

where λ is given by (3.1) and S is the set of places v for which $I_v(\mathcal{B}) > 0$ for some $\mathcal{B}$.

Now we note that by (3.1) the set $\mathcal{S}_0$ is not a union of components $\mathcal{B}$ of $\mathcal{S}$. Therefore, for every $v \in S$ there is a block $\mathcal{B}(v)$, possibly depending on v, containing an element $\sigma \in \mathcal{S}_0$ and another element $\tau \notin \mathcal{S}_0$. By Lemma 1, we then have $v(m_\sigma) = M$ and $v(m_\tau) < M - \lambda$, where λ is given by (1.4). It follows that $I_v(\mathcal{B}(v)) > \lambda$ and

$$\sum_{\mathcal{B}} \sum_{v} I_v(\mathcal{B}) \geq \sum_{v} I_v(\mathcal{B}(v)) > \lambda \cdot |S|.$$

This contradicts (3.5) and completes the proof of Theorem 1.

4. Proof of Theorems 2 and 3. Theorem 2 is a special case of Theorem 3.

Proof of Theorem 3. Let $I \subseteq \{1, \dots, n\}$ be a maximal subset of indices such that the elements α_i, $i \in I$, are pairwise non-proportional. Then every α_j is proportional to some α_i with $i \in I$ and equation (1.2) can be rewritten as

$$\sum_{i \in I} b_i(m) \alpha_i^m = 0 \tag{4.1}$$

where now

$$b_i(z) = \sum_{j:\, \alpha_j/\alpha_i \in k^*} a_j(z) (\alpha_j/\alpha_i)^z$$

is an exponential polynomial with characteristic roots α_j/α_i in k^* and coefficients in $K[z]$.

Let $\delta = d/dt$ be the usual derivation in $K := k(t)$ with field of constants k. We also want to describe the action of δ on exponential polynomials. To this end, we introduce indeterminates z and u_i, $i \in I$, algebraically independent over K and extend δ to the field $F = K(z, \{u_i : i \in I\})$ by means of

$$\delta(z) = 0, \qquad \delta u_i = z \delta(\alpha_i) \alpha_i^{-1} u_i,$$

so that u_i can be viewed as a formal exponential α_i^z on which δ acts by the chain rule. We denote by F_0 the field of constants of δ in F; it is clear that $k(z) \subseteq F_0$.

Let M_i, $i \in I$, be the $k[z]$-module generated by the coefficients $a_j(z)$ with $\alpha_j/\alpha_i \in k^*$. Since $k[z]$ is a principal ideal domain, M_i is free and there is a basis c_{ih}, $h = 1, \dots, h_i$, of this module such that

$$\sum_{h=1}^{h_i} \deg(c_{ih}(z)) \leq \sum_{j:\, \alpha_j/\alpha_i \in k^*} \deg(a_j(z)). \tag{4.2}$$

A proof of this statement is readily obtained following the proof of Corol-

lary 2 of Ch. I, Th. 1, p. 13 of Cassels [Ca]. It is also obvious that

$$N := \sum_{i \in I} h_i \le n. \tag{4.3}$$

With respect to this basis we have

$$b_i(z) = \sum_{h=1}^{h_i} c_{ih}(z) g_{ih}(z) \tag{4.4}$$

for suitable exponential polynomials $g_{ih}(z)$ with characteristic roots in k^* and coefficients in $k[z]$; the point of this decomposition is that now $\delta(g_{ih}(z)) = 0$ for every i, h. Moreover, (4.2) shows that

$$\sum_{i \in I} \sum_{h=1}^{h_i} \deg(c_{ih}(z)) \le \sum_{j=1}^{n} \deg(a_j(z)). \tag{4.5}$$

If we define $c_{lih}(z)$ by

$$c_{lih}(z) u_i = \delta^l(c_{ih} u_i) \tag{4.6}$$

and apply δ^l to (4.1) we obtain

$$\sum_{i \in I} \sum_{h=1}^{h_i} c_{lih}(m) g_{ih}(m) \alpha_i^m = 0. \tag{4.7}$$

The polynomials $c_{lih}(z)$ can be defined inductively directly in $K(z)$ by

$$c_{0ih}(z) = c_{ih}, \qquad c_{l+1,ih}(z) = \delta(c_{lih}(z)) + z\delta(\alpha_i)\alpha_i^{-1} c_{lih}(z).$$

Consider (4.7) for $l = 0, \dots, N-1$. This is a homogeneous linear system of N equations with a solution $g_{ih}(m)\alpha_i^m$, where the pairs (i, h) are indexed by $i \in I$ and, for fixed i, by $h = 1, \dots, h_i$. We have two cases.

Case I: *Every* $g_{ih}(m) = 0$. Such a solution is isotrivial by definition and is not part of the counting of solutions in Theorem 3.

Case II: *Some* $g_{ih}(m) \neq 0$. In this case the linear system of equations has a non-trivial solution. We define

$$R(z) := \det(c_{lih}(z))$$

where the rows are indexed by $l = 0, \dots, N-1$ and the columns by pairs (i, h) with $i \in I$ and, for each i, $h = 1, \dots, h_i$. Then we obtain $R(m) = 0$. Since $\deg(c_{lih}(z)) \le \deg(c_{ih}(z)) + h$, we see that $R(z)$ is a polynomial in $K[z]$ of degree at most

$$\sum_{i \in I} \sum_{h=1}^{h_i} \deg(c_{ih}(z)) + N(N-1)/2.$$

In particular, by (4.5) and (4.6) the number of roots does not exceed $d_1 + \ldots + d_n + n(n-1)/2$; therefore, if $R(z)$ is not identically 0 we have the conclusion of Theorem 3.

Thus we may assume that $R(z)$ is identically 0. By (4.6), we have

$$R(z) = \Big(\prod_{i\in I} u_i^{-h_i}\Big) \det(\delta^l(c_{ih}(z)u_i))$$

hence the identical vanishing of $R(z)$ is the same as the vanishing of the Wronskian of $c_{ih}(z)u_i$ with respect to the derivation δ. By the theorem of the Wronskian, this happens if and only if the elements $c_{ih}(z)u_i$ are linearly dependent over the field F_0 of constants of the derivation δ.

Now we claim that the elements u_i are linearly independent over the field $F_0(t)$ (note that $F_0(t) = K(z)F_0$ because $k(z) \subseteq F_0$). Suppose this is not the case and consider a non-trivial linear relation of smallest length

$$\sum \gamma_i u_i = 0$$

with $\gamma_i \in F_0(t)$. We apply δ to this relation and obtain a new relation

$$\sum (\delta(\gamma_i) + z\delta(\alpha_i)\alpha_i^{-1}\gamma_i)u_i = 0,$$

again with coefficients in $F_0(t)$. This relation must be proportional to the first relation and we conclude that

$$\lambda\gamma_i = \delta(\gamma_i) + z\delta(\alpha_i)\alpha_i^{-1}\gamma_i$$

for some $\lambda \in F_0(t)$, for at least two indices $i \in I$. If we eliminate λ, we see that there are two distinct indices $i, j \in I$ such that

$$\frac{\delta(\gamma_i/\gamma_j)}{\gamma_i/\gamma_j} + z\,\frac{\delta(\alpha_i/\alpha_j)}{\alpha_i/\alpha_j} = 0. \tag{4.8}$$

Let $\overline{F}_0$ be an algebraic closure of F_0 and look at the decomposition of (4.8) in partial fractions in the purely transcendental extension $\overline{F}_0(t)$ of $\overline{F}_0$; the derivation δ extends uniquely to $\overline{F}_0(t)$, with $\overline{F}_0$ its field of constants. The residue of any element $\delta(f)/f$, $f \in \overline{F}_0(t)$, at any point in $\overline{F}_0$ is an integer; since z is transcendental over $\mathbb{Q}$, we must have $\delta(\alpha_i/\alpha_j) = 0$. This is impossible, because α_i and α_j are non-proportional.

Thus we see that a linear dependence relation of the elements $c_{ih}(z)u_i$ over F_0 implies a linear dependence relation of the elements $c_{ih}(z)$ over F_0, for some fixed i and $h = 1, \ldots, h_i$. On the other hand, since $c_{ih}(z) \in K(z)$, another application of the Wronskian theorem shows that this relation already occurs in the field of constants of the derivation δ in the subfield $K(z) = k(z,t)$ of F. Since $k(z) \subseteq F_0$ and t is transcendental over F_0 we obtain a relation over $k(z)$. This contradicts the fact that the elements $c_{ih}(z)$ are a basis of the free $k[z]$-module M_i.

We conclude that $R(z)$ is not identically 0 and, with it, the proof of Theorem 3.

5. Concluding remarks. We conclude with two simple remarks. The first, which we owe to W. M. Schmidt, pertains to the equation

$$\sum_{j=1}^{n} a_j(m)\alpha_j^m \in k, \tag{5.1}$$

more general than (1.2). However, applying δ to this equation we find the new equation

$$\sum_{j=1}^{n} A_j(m)\alpha_j^m = 0, \tag{5.2}$$

with

$$A_j(z) = \delta(a_j(z)) + z\delta(\alpha_j)\alpha_j^{-1}a_j(z),$$

to which we may apply Theorem 3. Conversely, any non-isotrivial solution of (5.2) yields a solution of (5.1). Thus Theorem 3 can be used to obtain information about equation (5.1).

The second remark is that our method can be used to obtain bounds for the number of non-isotrivial solutions of (1.2) which depend solely on the number ν of monomials appearing in the polynomials $a_j(z)$, rather than their degree. We follow again the same proof as in Theorem 3, except that this time M_i is the k-vector space generated by the coefficients of the polynomials $a_j(z)$ with $\alpha_j/\alpha_i \in k^*$, rather than the $k[z]$-module generated by the polynomials themselves. Hence the quantity N is replaced by the ν, the total number of monomials appearing in (1.2). Again, we obtain a polynomial $R(z)$ vanishing at the non-isotrivial solutions of (1.2) and the same proof shows that it does not vanish identically. The degree of $R(z)$ is majorized by $\nu(\nu-1)/2$ and the same bound holds for the number of non-isotrivial solutions of (1.2).

References

[Be] F. Beukers, *The zero-multiplicity of ternary recurrences*, Compositio Math. 77 (1991), 165–177.

[BoM1] E. Bombieri and J. Mueller, *Trinomial equations in function fields*, Astérisque 228 (1995), 19–40.

[BoM2] —, —, *On a conjecture of Siegel*, Monatsh. Math. 125 (1998), 293–308.

[BrM] D. Brownawell and D. Masser, *Vanishing sums in function fields*, Math. Proc. Cambridge Philos. Soc. 100 (1986), 427–434.

[CHM] L. Caporaso, J. Harris and B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. 10 (1997), 1–35.

[Ca] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, 2nd printing, Springer, Berlin, 1971.

[SSW] H. P. Schlickewei, W. M. Schmidt and M. Waldschmidt, *Zeros of linear recurrences*, Manuscripta Math. 98 (1998), 225–241 .

[Schm] W. M. Schmidt, *The zero multiplicity of linear recurrence sequences*, Acta Math. 182 (1999), 243–282.

[V] F. Voloch, *Diagonal equations over function fields*, Bol. Soc. Brasil. Mat. 16 (1985), 29–39.

Institute for Advanced Study
School of Mathematics
Princeton, NJ 08540, U.S.A.
E-mail: eb@math.ias.edu

Department of Mathematics
Fordham University
Bronx, NY 10458, U.S.A.
E-mail: maiyu@cuphyb.phys.columbia.edu

Istituto Universitario di Architettura, DCA
Santa Croce 191
30135 Venezia, Italy
E-mail: zannier@iuav.unive.it

Received on 20.3.2000
and in revised form on 6.9.2000 (3783)