

# The Generalized Fermat Equation in Function Fields

E. BOMBIERI AND J. MUELLER\*

*School of Mathematics, Institute for Advanced Study,  
Princeton, New Jersey 08540; and  
Department of Mathematics, Fordham University,  
Bronx, New York 10458*

*Communicated by Hans Zassenhaus*

Received January 19, 1990; revised June 7, 1990

We show that if  $r > n!(n! - 2)$  the set of solutions  $x_j \in \mathbf{C}(t)$  of a Fermat equation  $\sum_1^n a_j x_j^r = 0$ ,  $a_j \in \mathbf{C}(t)$ , is the union of at most  $n!^{n!}$  families with an explicitly given simple structure. In particular, the number of projective solutions, up to  $r$ th roots of unity, of such an equation is either at most  $n!^{n!}$  or infinite. The proof uses the function field version of the *abc*-conjecture due to Mason, Voloch, and Brownawell and Masser. © 1991 Academic Press, Inc.

## I. INTRODUCTION

The purpose of this paper is to study the structure of the set of solutions of the generalized Fermat equation

$$a_1 z_1^r + a_2 z_2^r + \cdots + a_n z_n^r = 0$$

over a field  $K = k(t)$  of rational functions of one variable, with constant field  $k$  algebraically closed of characteristic 0. In practice, it is more convenient to deal with the linear equation

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 0$$

with coefficients  $a_i \in K$ , not all zero, and ask for solutions  $\mathbf{x}$  such that every coordinate  $x_i$  is an  $r$ th power.

Questions of this type have been studied by several authors. Bounds for the height and number of solutions as a function of the degree  $r$  and of the heights of the coefficients  $a_i$  of the basic Fermat equation can be found, for instance, in papers by Silverman [Sil] and Voloch [V]. Both authors rely on the so-called *abc*-conjecture of Masser and Oesterlé in function fields,

\* Supported in part by NSF Grant DMS-8808398.

proved by Mason [Ma], Voloch [V], and Brownawell and Masser [Br-M]; some of these ideas also appear in the book by Shafarevich [Sh, pp. 7-8], in the analysis of the classical Fermat equation in the function field case.

More recently, one of the authors of this paper [M] obtained results independent of the coefficients  $a_i$  in the case  $n=3$ , by noting that if there are sufficiently many solutions then one can eliminate the coefficients. The resulting vanishing determinant in the solutions is a Fermat equation with coefficients  $\pm 1$ , in a higher number of variables, and the  $abc$ -inequality can be used again. This idea of eliminating the coefficients appears explicitly in a short paper by Chowla [Ch] in 1964, although its origin may be earlier and possibly goes back to Siegel.

As a consequence, Mueller proved that a "non-degenerate" equation  $ax + by = c$  has at most two non-zero solutions  $x, y \in K^r$  if  $r > 30$ , which is clearly best possible except for the fact that the range for  $r$  can probably be diminished somewhat. She also deals with the case in which the function field  $K$  is a function field of one variable of positive genus, with rather similar results.

It is clear that in the study of the general Fermat equation one must allow infinite families of solutions. In fact the equation may split into smaller Fermat equations and moreover a Fermat equation, after a change of variable, may become equivalent to the equation  $z_1^r + \dots + z_n^r = 0$ , which we can solve easily with  $z_i \in k$ , since  $k$  is algebraically closed.

Our main result is that if  $r > r(n)$  then solutions fall into finitely many families with the simple structure described before and moreover there is a bound on the number of such families, as a function of  $n$  only.

**THEOREM.** *Suppose that  $r > n!(n! - 2)$ . Then the solutions of*

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = 0 \quad (1)$$

*with all  $x_i$ 's  $r$ th powers in  $K$  forming a finite number of families. Each family of solutions determines a decomposition*

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = \sum_{\mathcal{A}} \left( \sum_{j \in \mathcal{A}} a_jx_j \right),$$

*where*

$$\sum_{j \in \mathcal{A}} a_jx_j = 0$$

*for every  $\mathcal{A}$ . The set of solutions of the latter equation belonging to the given family consists of all points*

$$x_j = \eta_j^r S^r v_j,$$

where the  $\eta_j$ 's are suitable fixed elements of  $K$ ,  $S$  is an arbitrary element of  $K$ , and the vector  $\mathbf{v}_{\mathcal{R}} = \{v_j \mid j \in \mathcal{R}\}$  runs over all elements of some vector subspace of the euclidean space  $\mathbf{E}^{\text{Card}(\mathcal{R})}(k)$ .

Moreover, the number of such families is at most  $n!^{n!}$ .

**COROLLARY.** *Suppose that  $r > n!(n! - 2)$ . Then the number of equivalence classes, up to  $r$ th roots of unity, of  $K$ -rational points of the projective Fermat variety*

$$a_1 z_1^r + \dots + a_n z_n^r = 0$$

is either at most  $n!^{n!}$  or infinite.

Thus our result may be considered an extension of Mueller's theorem to a Fermat equation in several variables. There is no question that our theorem admits an extension to the case of a function of positive genus, and it is very likely that it may be generalized to deal with a large class of "fewnomial" equations. It is also clear that the method of proof will extend, with minor changes, to the case of number fields as soon as the appropriate form of the *abc*-conjecture is available.

We leave these generalizations aside for further study and limit ourselves here, mainly for the sake of simplicity, to the case of the generalized Fermat equation in dimension  $n$  over the function field  $K = k(t)$  with  $k$  algebraically closed of characteristic 0.

The authors thank A. Granville for pointing out an improvement of our original lower bound for  $r$  and W. M. Schmidt for some important suggestions.

## II. THE TRANSFORMED EQUATION

Let us consider the basic equation

$$a_1 x_1 + a_2 x_2 + \dots + a_n x_n = 0 \tag{1}$$

to be solved for  $x_i \in K^r$  and its set  $\mathcal{X}$  of solutions  $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \dots$ . We may also consider (1) as a set of linear equations for the quantities  $a_1, a_2, \dots$ , one for each solution  $\mathbf{x}^{(i)}$ . Since not all  $a_i$  are zero, we must have

$$\text{rank}(\mathbf{x}^{(i)})_{i=1,2,\dots} = m < n.$$

By reordering the solutions, we may also assume that

$$\text{rank}(\mathbf{x}^{(i)})_{i=1,2,\dots,m} = m < n$$

and thus

$$\text{rank}(\mathbf{x}^{(i)})_{i=1,2,\dots,m,v} = m < n \quad (2)$$

for every  $v$ .

Let  $J$  be any subset of  $\{1, \dots, n\}$  of cardinality  $|J| = m + 1$ . Then Eq. (2) yields

$$\det(\mathbf{x}_J^{(i)})_{i=1,2,\dots,m,v} = 0,$$

where, for a vector  $\mathbf{x}$ , we write  $\mathbf{x}_J = \{x_j | j \in J\}$ . If we expand the determinant in full we obtain

$$\sum_{\sigma} \varepsilon(\sigma) x_{\sigma_1}^{(1)} \cdots x_{\sigma_m}^{(m)} x_{\sigma_{m+1}}^{(v)} = 0, \quad (3)$$

where  $\sigma$  runs over the permutations of  $J$  and where  $\varepsilon(\sigma)$  is  $\pm 1$  according to the parity of  $\sigma$ . We abbreviate

$$m_{\sigma}(\mathbf{x}) = \varepsilon(\sigma) x_{\sigma_1}^{(1)} \cdots x_{\sigma_m}^{(m)} x_{\sigma_{m+1}}^{(v)};$$

denote by  $L_J$  the linear forms in  $x_1, \dots, x_n$ ,

$$L_J(x) = \sum_{\sigma} m_{\sigma}(\mathbf{x});$$

and denote by  $\mathcal{M} = \mathcal{M}(J)$  the set of permutations  $\sigma$  of  $J$ .

Some of the linear forms  $L_J$ , but not all, may be identically 0.

Our first and easy remark is that the system  $L_J(\mathbf{x}) = 0$  for varying  $J$  but fixed  $x^{(i)}$  is equivalent to Eq. (1).

LEMMA 1. *A vector  $\mathbf{x}$  with  $x_i \in K^r$  satisfies the Fermat equation*

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 0$$

*if and only if it satisfies the system of equations*

$$L_J(\mathbf{x}) = 0$$

*for every subset  $J \in \{1, \dots, n\}$  of cardinality  $m + 1$ .*

*Proof.* We have already shown that the solutions of the generalized Fermat equation (1) satisfy

$$L_J(\mathbf{x}) = 0$$

for every subset  $J \in \{1, \dots, n\}$  of cardinality  $m + 1$ .

In order to prove the implication in the other direction, we proceed as follows. Let  $V$  be the  $K$ -vector space of solutions of Eq. (1) but without the condition  $x_i \in K'$ . Then  $V$  has dimension  $n-1$  with a basis  $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(m)}, \mathbf{z}^{(1)}, \dots, \mathbf{z}^{(n-1-m)}$  for suitable vectors  $\mathbf{z}^{(h)}$ . Now the  $a_i$ 's are Grassmann coordinates for  $V$  and therefore they are proportional to the cofactors of the matrix of vectors of the basis. This means that there is  $\alpha \in K$  such that

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = \alpha \det \begin{pmatrix} \mathbf{x}^{(i)} \\ \mathbf{z}^{(h)} \\ \mathbf{x} \end{pmatrix}_{i=1, \dots, m; h=1, \dots, n-m-1}$$

We expand the right-hand side of this equation according to the Laplace expansion for the block of rows containing the auxiliary vectors  $\mathbf{z}^{(h)}$ , thus expressing  $a_1x_1 + a_2x_2 + \dots + a_nx_n$  as a linear combination of the  $L_J(\mathbf{x})$ ; this completes the proof of Lemma 1.

### III. APPLICATION OF THE *abc*-INEQUALITY

We are interested in which subsums in the left-hand side of (3) may vanish. Let

$$\sum_{\mathcal{A}} \left( \sum_{\mathcal{V}} m_{\sigma}(\mathbf{x}^{(v)}) \right) = 0$$

be a decomposition of (3) into vanishing subsums. This decomposition always exists, though it need not be unique. We may and do assume that every component

$$\sum_{\mathcal{A}} m_{\sigma}(\mathbf{x}^{(v)})$$

of the above sum has the property that no proper subsum of it vanishes.

For every decomposition as above there is a corresponding partition  $\pi = \bigcup \mathcal{N}$  of  $\mathcal{M}$  into subsets, and we group together solutions which give rise to the same partition. We also write  $\mathcal{M}(J)$  and  $\pi(J)$  if we want to emphasize the fact that these objects are associated with the set  $J$ .

DEFINITION. The set  $\mathcal{X}(\pi)$  is the set of solutions  $\mathbf{x} \in (K')^n$  such that

$$\sum_{\mathcal{A}} m_{\sigma}(\mathbf{x}) = 0 \tag{4}$$

for every component  $\mathcal{N}$  of the partition  $\pi$  and such that no proper of the above sum vanishes.

Now we can state

LEMMA 2. *Let  $J$  and  $\pi$  be as above. If  $r > n!(n! - 2)$  then for every solution  $\mathbf{x} \in \mathcal{X}(\pi(J))$  and every  $\sigma \in \mathcal{N}$  we have*

$$m_\sigma(\mathbf{x}) = \varepsilon(\sigma) x_{\sigma_1}^{(1)} \cdots x_{\sigma_m}^{(m)} x_{\sigma_{m+1}} = u_\sigma S^r, \tag{5}$$

where  $u_\sigma \in k$  depends on  $\sigma, \mathbf{x}, \mathcal{N}$ , while  $S \in K$  depends only on  $\mathbf{x}$  and  $\mathcal{N}$  but not on  $\sigma$ . Moreover we have

$$\sum_{\mathcal{N}} u_\sigma = 0 \tag{6}$$

and no proper subsum of the  $u_\sigma$ 's vanishes.

Conversely, suppose we are given the solutions  $\mathbf{x}^{(i)}, i = 1, \dots, m$ , and, for each  $J$ , let us choose a partition  $\pi$  of the set  $\mathcal{M}$  of the permutations of  $J$  into subsets  $\mathcal{N}$ . Suppose that for each  $J, \pi, \mathcal{N}$  and  $\sigma \in \mathcal{N}$  the point  $\mathbf{x}$  satisfies (5) and (6) for some  $u_\sigma \in k$  and some  $S \in K$ , independent of  $\sigma$ . Then  $\mathbf{x} \in \mathcal{X}$ .

*Proof.* Let  $\mathbf{x} \in \mathcal{X}(\pi)$ . We analyze (4) for each  $\mathcal{N}$ ; we need only consider the case in which  $N = \text{card}(\mathcal{N}) > 1$ . Each monomial  $m_\sigma(\mathbf{x})$  is a rational function of  $t$  and we can write

$$m_\sigma(\mathbf{x}) = P_\sigma R$$

for  $\sigma \in \mathcal{N}$ , where  $R$  is a non-zero rational function and where the  $P_\sigma$ 's are polynomials without common factor. Thus we have

$$\sum_{\sigma \in \mathcal{N}} P_\sigma = 0, \tag{7}$$

the elements of (7) are polynomials without common factor, and no subsum of (7) vanishes.

Let  $D_\sigma = \text{deg } P_\sigma$  and  $D = \max D_\sigma$  and let us choose  $\sigma_0$  such that  $D_{\sigma_0} = D$ . We define  $f_\sigma = P_\sigma / P_{\sigma_0}$  and apply Theorem B of [Br-M], i.e., the *abc*-inequality in function fields, to the sum  $\sum f_\sigma$ . We deduce

$$D \leq \sum_v (\gamma_N - \gamma_{m_v}),$$

where  $\gamma_p = (p - 1)(p - 2)/2$  and where, for each place  $v$  of  $K/k$ ,

$$m_v = \# \{ \sigma \mid f_\sigma \text{ is a unit at } v \}.$$

We write  $m_v = N - p_v$  and obtain a fortiori

$$D \leq \sum_v ((2N - 3) p_v - p_v^2)/2 \leq (N - 2) \sum_v p_v.$$

Suppose first that  $v \neq \infty$ . Then  $f_\sigma$  is a unit at  $v$  unless either  $P_\sigma$  or  $P_{\sigma_0}$  vanishes at  $v$ . Thus

$$\sum_{v \neq \infty} p_v \leq \sum_\sigma \# \{ \text{roots of } P_\sigma \text{ counted without multiplicity} \}.$$

For the place at  $v = \infty$  we note that  $f_\sigma$  is a unit unless  $D_\sigma < D$ . Thus

$$p_\infty \leq \# \{ \sigma \mid D_\sigma < D \}.$$

On the other hand, the coordinates of each element of  $\mathcal{X}$  are  $r$ th powers; therefore so are the monomials  $m_\sigma$  and the polynomials  $P_\sigma$  and the common factor  $R$ . In particular  $R = S^r$  for some  $S \in K$ .

Since every root of  $P_\sigma$  has multiplicity at least  $r$ , we have

$$\sum_\sigma \# \{ \text{roots of } P_\sigma \text{ counted without multiplicity} \} + \# \{ \sigma \mid D_\sigma < D \} \leq ND/r.$$

We combine this inequality with the two preceding inequalities and the bound on  $D$  and obtain

$$\max \deg P_\sigma \leq \frac{N(N - 2)}{r} \max \deg P_\sigma.$$

Also  $N \leq (m + 1)! \leq n!$ . Now we have two possibilities. If  $\max \deg P_\sigma > 0$  we deduce  $r \leq N(N - 2)$ , contrary to our hypothesis bounding  $r$  from below. Therefore  $\max \deg P_\sigma = 0$ , and we let each  $u_\sigma$  be the non-zero constant  $P_\sigma$ , which proves (5). It is also clear that (6) is equivalent to (4).

It remains to prove the last part of Lemma 2. The hypothesis  $\sum_{\mathcal{N}} u_\sigma = 0$  implies  $\sum_{\mathcal{N}} m_\sigma(\mathbf{x}) = 0$  for every component  $\mathcal{N}$  of the partition of  $\mathcal{M}$ , and therefore we also have  $L_J(\mathbf{x}) = 0$ . Since this holds for every  $J$ , the result follows from Lemma 1.

#### IV. PARAMETRIZATION OF SOLUTIONS AND CONCLUSION OF PROOF

In this section we simplify the parametrization of solutions obtained in Lemma 2 on the assumption that  $r > n!(n! - 2)$ .

According to Lemma 2, the solutions of (1) are obtained as follows. We start by choosing once and for all a basic set  $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(m)}$  of independent solutions. Then we choose, for every subset  $J \in \{1, \dots, n\}$  of cardinality

$m + 1$ , a partition  $\pi = \pi(J)$  of the set  $\mathcal{M}$  of permutations of  $J$ . Now suppose that for every component  $\mathcal{N}$  of the partition we have  $S \in K$  and  $u_\sigma \in k$  such that

$$m_\sigma(\mathbf{x}) = \varepsilon(\sigma) x_{\sigma_1}^{(1)} \cdots x_{\sigma_m}^{(m)} x_{\sigma_{m+1}} = u_\sigma S^r, \tag{5}$$

and moreover

$$\sum_{\sigma \in \mathcal{N}} u_\sigma = 0, \tag{6}$$

where also no proper subsum of (6) vanishes, and in particular,  $u_\sigma \neq 0$  if  $\text{Card}(\mathcal{N}) > 1$ . Then  $\mathbf{x} \in \mathcal{X}$  and every solution of (1) with all coordinates  $r$ th powers arises in this fashion for some collection of partitions  $\{J, \pi(J)\}$ .

The trouble with this parametrization is that different  $\sigma$ 's, perhaps associated to different components  $\mathcal{N}$  and different  $J$ 's, may involve the same  $x_{\sigma_{m+1}}$ , and our final step consists in analyzing how this can happen.

We begin with the case in which there are two or more  $\sigma$ 's with the same last coordinate  $\sigma_{m+1}$  and belonging to the same component  $\mathcal{N}$ . Let  $\sigma$  and  $\tau$  be two such elements and let us write for simplicity  $j = \sigma_{m+1} = \tau_{m+1}$ . Then (5) yields

$$\varepsilon(\sigma) x_{\sigma_1}^{(1)} \cdots x_{\sigma_m}^{(m)} x_j / u_\sigma = \varepsilon(\tau) x_{\tau_1}^{(1)} \cdots x_{\tau_m}^{(m)} x_j / u_\tau,$$

and thus, after division by  $x_j$ ,

$$\frac{u_\tau}{u_\sigma} = \frac{\varepsilon(\tau) x_{\tau_1}^{(1)} \cdots x_{\tau_m}^{(m)}}{\varepsilon(\sigma) x_{\sigma_1}^{(1)} \cdots x_{\sigma_m}^{(m)}}.$$

The right-hand side of this equation is independent of  $\mathbf{x}$ , while the left-hand side is an element of  $k$ . Therefore their common value must be a constant in  $k$  and we can write

$$u_\tau = \gamma_{\sigma, \tau} u_\sigma \tag{8}$$

for a constant  $\gamma_{\sigma, \tau} \in k$ , independent of  $\mathbf{x}$ .

Let  $p(\mathcal{N})$  be the image of the projection of  $\mathcal{N}$  into  $J$  obtained by means of the last coordinate, i.e.,  $\sigma \mapsto \sigma_{m+1}$ . We have shown:

LEMMA 3. *The set of Eqs. (5) and (6) for  $\sigma \in \mathcal{N}$  is equivalent to*

$$x_j = \eta_j^r S^r v_j \tag{9}$$

for  $j \in p(\mathcal{N})$ , where the  $\eta_j$ 's are independent of  $\mathbf{x}$  and where the  $v_j$ 's are elements of  $k$  satisfying a suitable linear condition

$$\sum_{j \in p(\mathcal{N})} c_j v_j = 0. \tag{10}$$

*Proof.* If  $\text{card}(\mathcal{N})=1$ , the result follows by taking  $c_j=1$  if  $x_{\sigma_1}^{(1)} \cdots x_{\sigma_m}^{(m)} \neq 0$ ,  $c_j=0$  otherwise, and  $\eta_j=1$ . If instead  $\text{card}(\mathcal{N})>1$ , it suffices to select one representative  $\sigma$  for each  $j \in p(\mathcal{N})$  and write  $v_j=u_\sigma$ ,  $\eta_j^r = (\varepsilon(\sigma) x_{\sigma_1}^{(1)} \cdots x_{\sigma_m}^{(m)})^{-1}$ . Now (8) shows that the linear condition (6) is equivalent to (10) for some constants  $c_j \in k$ , which concludes the proof.

We deal with the case of different components  $\mathcal{N}$ ,  $\mathcal{N}'$  with  $p(\mathcal{N}) \cap p(\mathcal{N}') \neq \emptyset$  in a similar fashion.

Let us say that  $p(\mathcal{N})$  and  $p(\mathcal{N}')$  are connected if they are not disjoint. Then the collection  $\{J, \pi(J)\}$  determines a partition  $\rho = \bigcup \mathcal{R}$  of  $\{1, \dots, n\}$  into maximal connected components of  $\bigcup \bigcup_{\pi(J)} p(\mathcal{N})$ .

LEMMA 4. *Let  $\{J, \pi(J)\}$  and  $\rho = \bigcup \mathcal{R}$  be as before. Then for every  $\mathcal{R}$  we can find elements  $\eta_j \in K$ ,  $j \in \mathcal{R}$  and a system of linear equations*

$$\sum_{j \in \mathcal{R}} c_{hj} v_j = 0 \tag{11}$$

with  $h = 1, \dots, h(\mathcal{R})$  and  $c_{hj} \in k$ , such that every  $\mathbf{x} \in \bigcap \mathcal{X}(\pi(J))$  is written as

$$x_j = \eta_j^r S^r v_j, \quad j \in \mathcal{R}, \tag{12}$$

for suitable  $S \in K$  and  $v_j \in k$  satisfying (11).

Conversely, if  $\mathbf{x}$  satisfies (11) and (12) with a vector  $\mathbf{v}_{\mathcal{R}} = \{v_j | j \in \mathcal{R}\}$ ,  $v_j \in k$ , and an element  $S_{\mathcal{R}} \in K$ , for all components  $\mathcal{R}$  of the partition  $\rho$ , then we have  $\mathbf{x} \in \mathcal{X}$ .

*Proof.* Let  $\mathcal{R}$  be a minimal connected component of the partition  $\rho$  and let  $R = \bigcup p(\mathcal{N}_\alpha)$ .

We order the sets  $p(\mathcal{N}_\alpha)$  so that each set  $p(\mathcal{N}_\alpha)$  is connected with at least one set preceding it and denote by  $\mathcal{R}_h$  the union of the first  $h$  elements of this ordering.

By Lemma 3, on each  $p(\mathcal{N}_\alpha)$  we have

$$x_j = \eta_{j\alpha}^r S_\alpha^r v_{j\alpha}, \quad j \in p(\mathcal{N}_\alpha),$$

with  $\eta_{j\alpha}$  independent of  $\mathbf{x}$  and with the  $v_{j\alpha}$  satisfying a linear relation

$$\sum_{p(\mathcal{N}_\alpha)} c_j(\mathcal{N}_\alpha) v_{j\alpha} = 0,$$

for suitable constants  $c_j(\mathcal{N}_\alpha) \in k$ .

We claim that the set of such equations corresponding to the first  $h$  elements of the ordering is equivalent to a system of relations

$$x_j = \eta_j^r S^r v_j, \quad j \in \mathcal{R}_h,$$

with  $\eta_j$  independent of  $x$  and with the  $v_j \in k$  satisfying  $h$  linear relations

$$\sum c_{ij} v_j = 0$$

for  $i = 1, \dots, h$ . The statement of Lemma 4 then is the statement corresponding to the last  $\mathcal{R}_h$  in the construction.

We prove our claim by induction on  $h$ . If  $h = 1$ , this is the conclusion of Lemma 3. Now suppose that  $h > 1$  and that the statement is true for  $h - 1$ , and hence

$$x_j = \eta_j^r S^r v_j, \quad j \in \mathcal{R}_{h-1}, \tag{13}$$

and

$$\sum c_{ij} v_j = 0$$

for  $i = 1, \dots, h - 1$ . To obtain the new system for  $\mathcal{R}_h$  we must add the new relations

$$x_j = \eta_{j\alpha}^r S_\alpha^r v_{j\alpha}, \quad j \in p(\mathcal{N}_\alpha), \tag{14}$$

and

$$\sum_{p(\mathcal{N}_\alpha)} c_j(\mathcal{N}_\alpha) v_{j\alpha} = 0 \tag{15}$$

associated to the  $h$ th element  $p(\mathcal{N}_\alpha)$  of the ordering.

By assumption, there is  $l \in \mathcal{R}_{h-1} \cap p(\mathcal{N}_\alpha)$ , and we choose  $l$  once and for all. Consider first the case in which  $\text{card}(\mathcal{N}_\alpha) = 1$ . Then Lemma 3 shows that either  $c_j(\mathcal{N}_\alpha) = 0$ , in which case (14) simply expresses the fact that  $x_j$  is an  $r$ th power, or  $c_j(\mathcal{N}_\alpha) \neq 0$ , in which case  $x_j = 0$  and therefore (15) can be expressed by the single equation  $v_j = 0$ . This shows that we need consider only the case in which  $\text{card}(\mathcal{N}_\alpha) > 1$ .

In this case, (13) and (14) yield

$$\eta_l^r S^r v_l = \eta_{l\alpha}^r S_\alpha^r v_{l\alpha}$$

and therefore

$$S_\alpha^r = \left( \frac{\eta_l}{\eta_{l\alpha}} \right)^r S^r \frac{v_l}{v_{l\alpha}}.$$

We substitute in (14), which then becomes

$$x_j = \left( \frac{\eta_l}{\eta_{l\alpha}} \eta_{j\alpha} \right)^r S^r \frac{v_l}{v_{l\alpha}} v_{j\alpha}, \quad j \in p(\mathcal{N}_\alpha). \tag{16}$$

Suppose first that  $j \in p(\mathcal{N}_x)$  but not  $j \in \mathcal{R}_{h-1}$ . Now we simply define  $\eta_j$  and  $v_j$  by means of

$$\eta_{jx} = \frac{\eta_{lx}}{\eta_l} \eta_j, \quad v_{jx} = \frac{v_{lx}}{v_l} v_j; \tag{17}$$

then (16) extends (13) to the whole of  $\mathcal{R}_h$ .

If instead,  $j \in p(\mathcal{N}_x) \cap \mathcal{R}_{h-1}$ , we analyze (16) as follows. By (13) and (16) we have

$$\eta_j^r S^r v_j = \left( \frac{\eta_l}{\eta_{lx}} n_{jx} \right)^r S^r \frac{v_l}{v_{lx}} v_{jx}$$

and therefore

$$\frac{v_l v_{jx}}{v_j v_{lx}} = \left( \frac{\eta_j \eta_{lx}}{\eta_l \eta_{jx}} \right)^r.$$

The right-hand side of this equation is independent of  $x$ , while the left-hand side is in  $k$ . Thus their common value is a constant  $\gamma_{jx} \in k$ . This means that

$$v_{jx} = \gamma_{jx} \frac{v_{lx}}{v_l} v_j \tag{18}$$

and

$$\eta_{jx} = \gamma_{jx}^{-1/r} \frac{\eta_{lx}}{\eta_l} \eta_j. \tag{19}$$

By (17), (18), (19) we see that if we define  $\gamma_{jx}$  to be 1 for  $j \in p(\mathcal{N}_x)$  but with  $j \notin \mathcal{R}_{h-1}$ , then (18) and (19) hold for every  $j \in p(\mathcal{N}_x)$ . Now Eq. (19) expresses compatibility relations which need to hold among the  $\eta_{jx}$ 's. We substitute (18) into (15) and obtain

$$\sum_{p(\mathcal{N}_x)} c_j(\mathcal{N}_x) \gamma_{jx} \frac{v_{lx}}{v_l} v_j = 0,$$

which, after division by  $v_{lx}/v_l$ , can be written as

$$\sum_{\mathcal{R}} c_{hj} v_j = 0$$

with  $c_{hj} = c_j(\mathcal{N}_x) \gamma_{jx}$  for  $j \in p(\mathcal{N}_x)$  and  $c_{hj} = 0$  elsewhere. This completes the induction step. The last part of Lemma 4 is also clear, since we take into

account relations (10) for all pairs  $\{J, \mathcal{N}\}$ , and thus Lemma 4 is established.

The proof of our theorem follows immediately from Lemma 4. In fact, each choice of a collection  $\{J, \pi(J)\}$  determines a family  $\bigcap_J \mathcal{X}(\pi(J))$  of solutions, which by Lemma 4 is parametrized as we want. Since

$$\mathcal{X} = \bigcap_J \mathcal{X}(\pi(J))$$

with  $\bigcup$  over all possible collections of partitions  $\{J, \pi(J)\}$ , a bound for the number of families is obtained by counting the number of choices for  $\{J, \pi(J)\}$ . For each  $J$  we have  $(m+1)^{(m+1)!}$  choices of  $\pi$ , and we have  $\binom{n}{m+1}$  possibilities for  $J$ . Thus the number of families of solutions is at most

$$\#\{\text{families}\} \leq ((m+1)^{(m+1)!})^{\binom{n}{m+1}} \leq n!^{n!} \leq n^n.$$

#### REFERENCES

- [Br-M] W. D. BROWNAWELL AND D. W. MASSER, Vanishing sums in function fields, *Math. Proc. Cambridge Philos. Soc.* **100** (1986), 427–434.
- [Ch] S. CHOWLA, Remarks on two theorems of Siegel, *Acta Arith.* **9** (1964), 417–418.
- [M] J. MUELLER, Binomial Thue's equation over function fields, *Compositio Math.* **73** (1990), 189–197.
- [Ma] R. C. MASON, Diophantine equations over function fields, in "London Math. Society Lecture Notes," Vol. 96, Cambridge Univ. Press, London/New York, 1984.
- [Sh] I. R. SHAFAREVICH, "Basic Algebraic Geometry," Springer-Verlag, Berlin/Heidelberg/New York, 1977.
- [Sil] J. H. SILVERMAN, The Catalan equation over function fields, *Trans. Amer. Math. Soc.* **273** (1982), 201–205.
- [V] J. F. VOLOCH, Diagonal equations over function fields, *Bol. Soc. Brasil. Math.* **16** (1985), 29–39.