Furstenberg theorem for systems of

JOURNAL OF ALGEBRA 7, 271-277 (1967) Polynomial equations?

Algebraic Functions over Finite Fields

HARRY FURSTENBERG*

Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem, Israel

Communicated by Nathan Jacobson

Received December 20, 1966

1. INTRODUCTION

Laurent series

If κ is a field, $\kappa((x))$ will denote the field of formal power series with coefficients in κ: $f \in \kappa((x))$ if $f = \sum_{-\infty}^{\infty} a_n x^n$, $a_n \in \kappa$, $a_n = 0$ for $n < -\mu$, $\mu < \infty$. By an *algebraic function over* κ we mean an element of $\kappa((x))$ which is algebraic over the field of rational functions $\kappa(x)$. Thus $x^{1/2}$ is not, in our terminology, an algebraic function. On the other hand,

for some μ

$$\sum_0^{\infty} \binom{2n}{n} x^n = \sum_0^{\infty} \binom{-\frac{1}{2}}{n} (-4)^n x^n = (1 - 4x)^{-1/2}$$

is an algebraic function with respect to any field. If κ has characteristic p, it is easy to construct numerous explicit examples of algebraic functions. For example, $f(x) = \sum_0^{\infty} x^{p^n}$ is algebraic, since

$$f(x) = x + f(x^p) = x + \{f(x)\}^p.$$

We are interested in properties of the coefficient sequences of algebraic functions. Let us say that a sequence of elements in κ, $\{a_n\}_{-\infty}^{\infty}$ is *algebraic over* κ if $\sum_{-\infty}^{\infty} a_n x^n$ is an algebraic function in $\kappa((x))$. If A_κ is the set of all algebraic sequences over κ, then A_κ obviously possesses a κ-linear structure, as well as a multiplicative structure given by convolution: $\{a_n\} * \{b_n\} = \{\sum_{m-\infty}^{\infty} a_{n-m} b_m\}$. On the other hand A_κ need not be closed with respect to ordinary multiplication: $\{a_n\}, \{b_n\} \to \{a_n b_n\}$. For example, if κ is the field of rationals, then the sequence $\{\binom{2n}{n}^2\}$ is not algebraic. In fact

$$\sum_0^{\infty} \binom{2n}{n}^2 x^n = \sum_0^{\infty} \binom{2n}{n} \left\{\frac{1}{2\pi} \int_{-\pi}^{\pi} (2 \cos \theta)^{2n} \, d\theta \right\} x^n$$
$$= \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{d\theta}{(1 - 16x \cos^2 \theta)^{1/2}},$$

* This research was supported in part by a grant from the Sloan Foundation and in part by the Office of Scientific Research of the Office of Aerospace Research of the USAF under Grant No. AF-AFOSR-381-63.

which cannot be an algebraic function of x. Indeed, according to [2, p. 62], the values of this function are *never* algebraic unless x is transcendental.

Our main result is that this phenomenon does not occur for finite fields.

THEOREM A. *If κ is a finite field, $\{a_n\}$, $\{b_n\}$ two algebraic sequences over κ, then $\{a_n b_n\}$ is again algebraic.*

Let us draw some simple consequences of Theorem A. Suppose we call a subset N of the non-negative integers *algebraic over* κ if $\sum_{n \in N} x^n$ is an algebraic function in $\kappa((x))$.

COROLLARY 1. *If κ is a finite field, then the family of algebraic subsets over κ is closed with respect to finite unions and intersections.*

COROLLARY 2. *If κ is finite, then a sequence $\{a_n\}$ is algebraic over κ if and only if $a_n = 0$ for n sufficiently negative, and, for each $b \in \kappa$, $\{n \geqslant 0 : a_n = b\}$ is an algebraic set.*

Corollary 1 is immediate and so is the sufficiency of the condition in Corollary 2. To see the necessity, let $\sum a_n x^n$ be algebraic, and suppose κ has q elements in it. Then, by Theorem A, $\sum_0^\infty \{1 - (a_n - b)^{q-1}\} x^n$ is algebraic, which is the desired result.

According to Corollary 2, the study of algebraic sequences over a finite field reduces to the study of the ring of algebraic sets with respect to the field. Let $F(q)$ denote the field with q elements. If a function $f \in F(p)((x))$ is algebraic over $F(p^m)(x)$, it is also algebraic over $F(p)(x)$. It follows that the Boolean ring R_{p^m} of algebraic sets over $F(p^m)$ depends only on the characteristic p. It would be of interest to determine the rings R_p explicitly. Note that finite unions of arithmetic progressions are in all R_p. It is quite likely that, modulo finite sets, these are the only sets common to all the R_p.

2. DIAGONALIZATION OF POWER SERIES

Let $f(x_1, x_2, \ldots, x_m)$ be a formal power series in m variables:

$$f(x_1, x_2, \cdots, x_m) = \sum_{n_i > -\mu} a_{n_1 n_2 \cdots n_m} x_1^{n_1} x_2^{n_2} \cdots x_m^{n_m}, \qquad a_{n_1 n_2 \cdots n_m} \in \kappa. \tag{1}$$

We denote by $\mathscr{D} f$ the formal power series in a single variable defined by

$$\mathscr{D} f(t) = \sum a_{nn \cdots n} t^n. \tag{2}$$

$\mathscr{D} f$ will be called the *diagonal* of f.

Suppose $m = 2$ and that κ is the field of complex numbers. We can then show that if f represents a rational function of two variables, then $\mathscr{D}f$ represents an algebraic function. For we have

$$(\mathscr{D}f)(t) = \frac{1}{2\pi i}\int_{|\zeta|=\epsilon} f\left(\zeta, \frac{t}{\zeta}\right)\frac{d\zeta}{\zeta} \tag{3}$$

for ϵ and $|t|$ sufficiently small so that $f(z, w)$ is regular for $|z| < \epsilon$, $|w| < t\epsilon^{-1}$. Now the integrand is rational, and evaluating it by residues clearly leads to an algebraic function of the variable t.

This argument fails when $m \geqslant 3$. To calculate the diagonal of a rational function of 3 variables, we must perform two contour integrations. The first leads to an algebraic function of two variables, and the contour integral of such an expression with respect to one of the variables is generally a transcendental function of the remaining variable. For example, the abelian integral

$$\omega(\gamma) = \int_\gamma \frac{d\zeta}{(\zeta^3 - \zeta - g_3)^{1/2}} \tag{4}$$

taken over a contour on the Riemann surface of the algebraic function in the integral, cannot depend algebraically on g_3. For, the variable g_3 itself is an automorphic function of $\tau = \omega(\gamma_1)/\omega(\gamma_2)$([1]). It is possible to show that (4) occurs as the diagonal of a rational function of three variables. → holonomic

Nonetheless, for fields of finite characteristic we have

THEOREM 1. *If the ground field κ has finite characteristic, then the diagonal of a rational function of several variables is an algebraic function of one variable.*

Proof. If ν is an integer vector, $\nu = (n_1, n_2, \dots, n_m)$, x^ν will denote the monomial $x_1^{n_1}x_2^{n_2}\cdots x_m^{n_m}$. We shall say that ν is homogeneous if $n_1 = n_2 = \cdots = n_m$ and we denote the common value by $\bar{\nu}$. Notice that if ν is homogeneous and $g = x^\nu f$, then $\mathscr{D}g(t) = t^{\bar{\nu}}\mathscr{D}f(t)$.

Let f be a rational function in m variables, $f(x) = P(x)/Q(x)$, and set $\varphi = \mathscr{D}f$. Clearly it will suffice to prove the theorem (that $\varphi = \mathscr{D}f$ is algebraic) in case $P(x)$ reduces to a monomial. Now we have

$$\mathscr{D}(x^\nu/Q(x)) = \mathscr{D}(x^{\nu+\mu}/x^\mu Q(x)),$$

so that if we choose μ such that $\nu + \mu$ is homogeneous, we see that we can reduce the general case to the case: $f(x) = Q(x)^{-1}$.

Write $Q(x) = \sum_{\nu\in L} a_\nu x^\nu$, where L is a set of non-negative integer vectors. Clearly there is no loss of generality if we take L to be all non-negative integer vectors less than (componentwise) some fixed vector λ. Let p denote the characteristic of κ. We have

$$\Big(\sum_L a_\nu x^\nu\Big)^{p-1} f^{p-1} = 1 \tag{5}$$

or

$$\Big(\sum_L a_\nu x^\nu\Big)^{p-1} f^p = f.$$

Let $\mu \in L$.

$$x^\mu f = x^\mu \Big(\sum_L a_\nu x^\nu\Big)^{p-1} f^p = \sum_{L^{p-1}} b_{\nu_1\nu_2\cdots\nu_{p-1}} x^{\nu_1+\nu_2+\cdots+\nu_{p-1}+\mu} f(x)^p. \tag{6}$$

The coefficients b are products of the a_ν. We reduce the exponents in (6) modulo p. That is, we write

$$\nu_1 + \nu_2 + \cdots + \nu_{p-1} + \mu = p\sigma(\nu_1, \nu_2 \cdots, \nu_{p-1}; \mu) + \rho(\nu_1, \nu_2, \ldots \nu_{p-1}; \mu),$$

where each component of ρ is between 0 and $p - 1$, and σ is a nonnegative-integer vector. Note that

$$\sigma \leqslant p^{-1}(\nu_1 + \nu_2 + \cdots + \nu_{p-1} + \mu) < p^{-1}p\lambda = \lambda$$

so that $\sigma \in L$.

We now rewrite (6) as

$$x^\mu f = \sum b_{\nu_1\nu_2\cdots\nu_{p-1}} x^{\rho(\nu_1,\nu_2,\cdots,\nu_{p-1},\mu)}\{x^{\sigma(\nu_1,\nu_2,\cdots\nu_{p-1};\mu)}f(x)\}^p. \tag{7}$$

Apply $\mathscr{D}$ to both sides of (7). In the expansion of $\{x^\tau f\}^p$ the only terms appearing are those with exponents divisible by p. To obtain a non-vanishing diagonal term in $x^\rho\{x^{\sigma f}\}^p$, inasmuch as the components of ρ are between 0 and $p - 1$, the vector ρ must be homogeneous. We then obtain

$$\begin{aligned}\mathscr{D}(x^\mu f) &= \sum{}' b_{\nu_1\nu_2\cdots\nu_{p-1}} t^{\beta(\nu_1,2,\cdots\nu_{p-1},\mu)}\mathscr{D}(\{x^{\sigma(\nu_1,\nu_2,\cdots,\nu_{p-1};\mu)}f(x)\}^p)\\ &= \sum{}' b_{\nu_1\nu_2\cdots\nu_{p-1}} t^\beta\{\mathscr{D}(x^\tau f(x))\}^p,\end{aligned} \tag{8}$$

where $\sum'$ indicates that the summation is carried over only a part of the original range.

Let $q_\mu(t) = \mathscr{D}(x^\mu f)$, $\mu \in L$. We have then shown that for each μ in L, there is an equation

$$\varphi_\mu(t) = \sum c_{\mu\nu}(t)\{\varphi_\nu(t)\}^p$$

where the $c_{\mu\nu}$ are polynomials in t. Now quite generally, if elements ξ_i, $i = 1,\ldots, n$ from an extension of a field K satisfy a system of equations $\xi_i = \sum_1^n c_{ij}\xi_j{}^p$, then the ξ_i are algebraic over K. This proves the theorem.

3. Converse of Theorem 1

As a matter of fact, every algebraic function comes about by the diagonalization procedure of the foregoing section. For the complex field this amounts to the assertion that every algebraic function in one variable is a contour integral of a rational function of two variables:

$$\varphi(z) = \int_\gamma R(z, w)\, dw. \tag{9}$$

In fact, if we suppose $\varphi(0) = 0$ and that φ satisfies the polynomial equation $P(z, \varphi(z)) = 0$, and that, in addition, 0 is an isolated root of $P(0, w) = 0$, then we can determine $R(z, w)$ explicitly as

$$\boxed{R(z, w) = w\frac{\partial P}{\partial w}(z, w)/P(z, w).} \tag{10}$$

Expressing (9) in the form (3), we see that we can obtain $\varphi(z)$ explicitly as the diagonal of a rational function of two variables. While this does not constitute a proof for fields other than the complex field, it provides us with an explicit formula which we may proceed to verify by some other means.

Proposition 1. *If $\varphi(x)$ is an algebraic function over a finite field, then $\varphi(x) = R(x) + x^h\psi(x)$, where $R(x)$ is a rational function, and $\psi(x)$ is algebraic, satisfying an equation of the form*

$$A_0(x)\psi(x) = A_1(x)\psi^p(x) + \cdots + A_n(x)\psi^{p^n}(x) + B(x), \tag{11}$$

where the $A_i(x)$ and $B(x)$ are polynomials and $A_0(x)$ is not divisible by x.

Proof. The functions $\varphi, \varphi^p, \varphi^{p^2},\ldots$ cannot be linearly independent over $\kappa(x)$, so there exists some relationship of the form

$$A_0'(x)\varphi^{p^l}(x) = A_1'(x)\varphi^{p^{l+1}}(x) + \cdots + A_n'(x)\varphi^{p^{l+n}}(x). \tag{12}$$

We wish to show that we can take $l = 0$. Assume to the contrary that $l > 0$. Then all the powers of φ occurring in (12) are functions of x^p. As a result, if x^i is a power of x that occurs in some $A_j'(x)$, and we strike out from each $A_m'(x)$ all the terms x^r for $r \not\equiv i \pmod p$, we must still have equality. Dividing

$y = xy^2+1$ $\quad P(x,y) = y-(xy^2+1)$

$P_y = 1-2xy$

$P_y(xy,y) = 1-2xy^2$

$$\boxed{\frac{y^2(1-2xy^2)}{y-(xy^3+1)}}$$

the resulting equation by x^i, we obtain another identity in which all the exponents of x are divisible by p. Now since the ground field is finite, every element in κ is a pth power, hence we can extract the pth root of the equation in question, thus obtaining an equation of the form (12), but with $l-1$ in the place of l.

Thus we may suppose that φ satisfies a relationship of the form

$$A_0''(x)\varphi(x) = A_1''(x)\varphi^p(x) + \cdots + A_n''(x)\varphi^{p^n}(x). \tag{13}$$

If $A_0''(x)$ is not divisible by x we are through. If $A_0''(x)$ is divisible by x^r, write $\varphi(x) = \varphi(0) + x\psi(x)$, assuming that the power series for φ has no negative exponents. Clearly, subtracting a rational function R, we may assume that this is the case. We then find

$$A_0''(x)x\psi(x) = A_1''(x)x^p\psi^p(x) + \cdots + A_n''(x)x^{p^n}\psi^{p^n}(x) + B''(x) \tag{14}$$

for an appropriate polynomial $B''(x)$. Let $s = \min(p, r+1)$. Each term $A_j''(x)x^{p^j}$ is divisible by x^s and so $B''(x)$ is also divisible by x^s. We may therefore divide (14) by x^s which yields an equation of the same form as (11), but for which the power of x dividing $A_0''(x)$ is, at most x^{r-1}. Iterating this procedure we obtain the proposition. $D\{\varphi(xy)\} = \varphi(x)$

$c_0 = 0$

* PROPOSITION 2. *Let $P(x,y)$ be a polynomial and $\varphi(x) = \sum_1^\infty c_n x^n$ a function in $\kappa((x))$ satisfying $P(x, \varphi(x)) = 0$. If $(\partial P/\partial y)(0,0) \neq 0$, then*

in fact in $K[[x]]$

$$\boxed{\varphi = \mathscr{D}\left\{y^2 \frac{\partial P}{\partial y}(xy, y)/P(xy, y)\right\}.}$$

Here κ is an arbitrary field.

$P_y(x,y) = Q(x,y) + (y-\varphi(x))\,Q_y(x,y)$

Proof. We write $P(x,y) = (y-\varphi(x))Q(x,y)$ with Q a polynomial in y whose coefficients are power series in x. We have $Q(0,0) \neq 0$, since $\varphi(0) = 0$. ?? Then

$$\frac{1}{P}\frac{\partial P}{\partial y}(x,y) = \frac{1}{y-\varphi(x)} + \frac{1}{Q}\frac{\partial Q}{\partial y}(x,y). \tag{15}$$

We now verify Proposition 2 by replacing x by xy in (15), multiplying by y^2 and forming the diagonal. We have

$$\mathscr{D}\left\{\frac{y^2}{y-\varphi(xy)}\right\} = \mathscr{D}\{y(1-y^{-1}\varphi(xy))^{-1}\} = \mathscr{D}\left\{\sum_0^\infty y^{-n+1}\varphi(xy)^n\right\}$$

$$= \mathscr{D}\{\varphi(xy)\} = \varphi.$$

$\frac{P_y}{P} = \frac{P_y}{(y-\varphi)Q} = \frac{1}{y-\varphi} + \frac{Q_y}{Q}$ $\Big|$ $\frac{y}{1-\frac{\varphi}{y}} = y\cancel{\varphi(xy)^0} + \varphi(xy)^1 + \cancel{y^{-1}\varphi(xy)^2} + \cdots$

under D

On the other hand, since $Q(0, 0) \neq 0$, the second term in (15) leads to a power series in xy and y. When we now multiply this by y^2, we find that there are no diagonal terms whatever. This proves the proposition.

THEOREM 2. *If $\varphi(x)$ is an algebraic function over a finite field, then $\varphi = \mathscr{D}(R(x, y))$ for a power series in two variables $R(x, y)$ that represents a rational function of x and y.*

Proof. Clearly we may suppose that the function φ has no negative exponents in its expansion, since, in any case there are at most a finite number of these. By Proposition 1, we may express φ in terms of a function ψ which again may be assumed to possess no negative exponents, and which satisfies (11). The function $\psi(x) - \psi(0)$ satisfies an equation of the same form, and, moreover, satisfies the conditions of Proposition 2. Hence $\psi(t) - \psi(0)$ is the diagonal of a rational function, and it follows immediately that the same is true for φ.

4. PROOF OF THEOREM A

Now let $\varphi(x) = \sum_{-\infty}^{\infty} a_n x^n$ and $\psi(x) = \sum_{-\infty}^{\infty} b_n x^n$ be two algebraic functions in $\kappa((x))$, κ a finite field. By Theorem 2,

$$\varphi = \mathscr{D}(R(x, y)), \qquad \psi = \mathscr{D}(S(z, w)),$$

where $R(x, y)$, $S(z, w)$ are rational functions. Form the function of four variables $H(x, y, z, w) = R(x, y)S(z, w)$ and let θ denote its diagonal. It is clear that $\theta(t) = \sum_{-\infty}^{\infty} a_n b_n t^n$. But by Theorem 1, $\theta(t)$ is an algebraic function, and this proves Theorem A.

Perhaps the main significance of these results is in pointing to what still remains to be done in the classical case of the complex field. Specifically, one would like to know which analytic functions occur as diagonals of rational functions of several variables. Since these are precisely the algebraic functions in the case of a finite field, they cannot be devoid of interest in the complex case. The integral in (4) indicates that, at least in certain cases, they are tied up with automorphic functions.

REFERENCES

1. COURANT, R. AND HURWITZ, A. "Funktionentheorie." Springer, Berlin, 1929.

2. SCHNEIDER, TH. "Einführung in die Tranzendenten Zahlen. Springer, Berlin, 1957.