Math. Proc. Camb. Phil. Soc. (2012), **153**, 235–247 © *Cambridge Philosophical Society* 2012
doi:10.1017/S0305004112000114
First published online 22 February 2012

On the set of zero coefficients of a function satisfying a linear differential equation

BY JASON P. BELL†

Department of Mathematics, Simon Fraser University, 8888 *University Dr., Burnaby, BC, V5A* 1*S6 Canada.*
e-mail: jpb@sfu.ca

STANLEY N. BURRIS

Department of Pure Mathematics, University of Waterloo, Waterloo, ON, N2L 3*G1, Canada.*
e-mail: snburris@math.uwaterloo.ca

AND KAREN YEATS

Department of Mathematics, Simon Fraser University, 8888 *University Dr., Burnaby, BC, V5A* 1*S6, Canada.*
e-mail: karen_yeats@sfu.ca

(*Received* 14 *June* 2011; *revised* 1 *November* 2011)

Abstract

Let K be a field of characteristic zero and suppose that $f : \mathbb{N} \to K$ satisfies a recurrence of the form

$$f(n) = \sum_{i=1}^{d} P_i(n) f(n-i),$$

for n sufficiently large, where $P_1(z), \ldots, P_d(z)$ are polynomials in $K[z]$. Given that $P_d(z)$ is a nonzero constant polynomial, we show that the set of $n \in \mathbb{N}$ for which $f(n) = 0$ is a union of finitely many arithmetic progressions and a finite set. This generalizes the Skolem–Mahler–Lech theorem, which assumes that $f(n)$ satisfies a linear recurrence. We discuss examples and connections to the set of zero coefficients of a power series satisfying a homogeneous linear differential equation with rational function coefficients.

1. *Introduction*

The Skolem–Mahler–Lech theorem is a well-known result that describes the set of solutions to an equation $f(n) = 0$, where $f(n)$ is a sequence given by a linear recurrence. Throughout this paper, we take $\mathbb{N} := \{0, 1, 2, \ldots\}$.

THEOREM 1·1 (Skolem–Mahler–Lech). *Let K be a field of characteristic zero and let $f : \mathbb{N} \to K$ be a sequence satisfying a linear recurrence over K; that is, a recurrence*

† The authors thank NSERC for supporting this project.

of the form $f(n) = \sum_{j=1}^{d} a_j f(n-j)$, *for* $n \geqslant d$, *with* $a_1, \ldots, a_d \in K$. *Then the set* $\{n \in \mathbb{N} : f(n) = 0\}$ *is a union of finitely many arithmetic progressions and a finite set.*

This theorem was first proved for linear recurrences over the rational numbers by Skolem [**32**], and it was then proved for linear recurrences over the algebraic numbers by Mahler [**22**]. The version above was proved first by Lech [**20**] and later by Mahler [**23**, **24**]. Further background about linear recurrences and the Skolem–Mahler–Lech theorem can be found in the book by Everest, van der Poorten, Shparlinski, and Ward [**13**]. There are many different proofs and extensions of the Skolem-Mahler-Lech theorem in the literature [**3**, **4**, **6**, **7**, **17**, **28**, **29**]—all known proofs of the Skolem–Mahler–Lech theorem use p-adic methods in some way, albeit sometimes in a disguised manner.

Recall that if K is a field, then $f : \mathbb{N} \to K$ satisfies a linear recurrence over K if and only if

$$\sum_{n=0}^{\infty} f(n) z^n \in K[[z]]$$

is the power series expansion of a rational function in $K(z)$. Stanley [**33**, theorem 2·1] shows that

$$\{\text{Rational power series}\} \subseteq \{\text{Algebraic power series}\} \subseteq \{\text{Differentiably finite power series}\}.$$

Algebraic power series comprise the power series $F(z) \in K[[z]]$ which satisfy a nonzero polynomial equation $P(z, F(z)) = 0$ with $P(z, y) \in K[z, y]$. The set of *differentiably finite* power series $F(z)$ are those that satisfy a non-trivial homogeneous linear differential equation with rational function coefficients:

$$\sum_{i=0}^{d} Q_i(z) \frac{d^i}{dz^i} F(z) = 0. \tag{1·1}$$

Definition 1·2. Let K be a field and let $f : \mathbb{N} \to K$ be a K-valued sequence. We say that $f(n)$ is *holonomic* if the power series

$$\sum_{n=0}^{\infty} f(n) z^n \in K[[z]]$$

is differentiably finite.

It is straightforward to show that a K-valued sequence $f(n)$ is holonomic if it satisfies a *polynomial-linear recurrence*; that is, there exist a natural number d and polynomials $P_0(z), \ldots, P_d(z) \in K[z]$, not all zero, such that

$$\sum_{i=0}^{d} P_i(n) f(n-i) = 0, \tag{1·2}$$

for all sufficiently large n (see Stanley [**33**, theorem 1·5]). It will be convenient to use this characterization of holonomic sequences throughout this paper.

Differentiably finite power series and holonomic sequences have been extensively studied by several authors [**10**, **11**, **15**, **16**, **33**, **35**], and many important sequences arising naturally in combinatorics, number theory, and algebra have been shown to be holonomic [**9**, **16**, **21**, **27**, **33**]. A number of significant results, including the following, have employed

holonomic methods: (i) Apéry's proof of the irrationality of $\zeta(3)$ used a sequence satisfying a polynomial-linear recurrence (see van der Poorten's survey [**27**]); (ii) Wilf and Zeilberger [**35**] showed how the theory of holonomic sequences could be applied to the "automatic" proving of combinatorial identities; and (iii) Bousquet–Mélou [**9**] applied the theory to enumeration of walks in the quarter plane.

In light of the well-behaved nature of the zero set of a sequence satisfying a linear recurrence over a field of characteristic zero, it is natural to ask whether a similar result holds for holonomic sequences. Indeed, Rubel [**31**, Problem 16] asked: *does the conclusion of the Skolem–Mahler–Lech theorem hold for all holonomic sequences?* The strongest result in this direction is due to Bézivin [**7**] and Methfessel [**26**]: the set of zeros of a holonomic sequence can be expressed as a union of finitely many arithmetic progressions and a set of zero density. (Bézivin assumed that 0 and ∞ are not irregular singular points of the corresponding linear differential equation.) Laohakosol [**19**] and Bézivin and Laohakosol [**8**] showed that the answer to Rubel's question is 'yes', provided additional technical conditions on the associated differential equation hold. (There is an error in the first paper of Laohakosol which is repaired in the subsequent paper with Bézivin.)

We are able to give an affirmative answer to Rubel's question in the case that the recurrence has a reciprocal property (see Stanley [**33**, section 3]), namely the recurrence can be 'run backwards' in a well-behaved way. We note that if K is a field and $f : \mathbb{N} \to K$ satisfies a polynomial linear recurrence

$$f(n) = \sum_{i=1}^{d} P_i(n) f(n-i)$$

with $P_1(z), \ldots, P_d(z)$ polynomials and $P_d(z)$ a nonzero constant then we may rewrite the recurrence as

$$f(n) = \sum_{i=1}^{d-1} \lambda P_{d-i}(n+d) f(n+i) - \lambda f(n+d),$$

where $\lambda = -1/P_d(z)$, a nonzero element of K. Thus the definition of $f(n)$ extends to all $n \in \mathbb{Z}$. The reciprocal property of Stanley mentioned above is given by the assumption that $P_d(z)$ is a nonzero constant polynomial.

THEOREM 1·3. *Let K be a field of characteristic zero, let d be a positive integer, and let $P_1(z), \ldots, P_d(z) \in K[z]$ be polynomials with $P_d(z)$ a nonzero constant. Suppose that $f : \mathbb{N} \to K$ is a sequence satisfying the polynomial-linear recurrence*

$$f(n) = \sum_{i=1}^{d} P_i(n) f(n-i) \tag{1·3}$$

for all n sufficiently large. Then $\{n \in \mathbb{N} : f(n) = 0\}$ is a union of finitely many arithmetic progressions and a finite set.

This theorem generalizes the Skolem–Mahler–Lech theorem, which asserts that the conclusion holds provided $P_1(z), \ldots, P_d(z)$ are constant polynomials.

We note that Lech [**20**] gave examples that showed that the conclusion of the Skolem-Mahler-Lech theorem does not hold if one eliminates the hypothesis that the field have characteristic 0. For example if p is a prime and $K = \mathbb{F}_p(t)$, then $f(n) = (1+t)^n - t^n - 1$ satisfies a linear recurrence over K but the zero set of f is $\{1, p, p^2, \ldots\}$. Derksen [**12**]

showed that the zero set $\mathcal{S}$ of a linear recurrence over a field of characteristic $p > 0$ has the property that there is a finite-state automaton which takes as input the base p expansion of a number n and accepts the number if and only if $n \in \mathcal{S}$. We call such sets *p-automatic sets* (see the book of Allouche and Shallit [**2**] for a more precise definition).

Recently, Adamczewski and the first-named author [**1**] have shown that the set of zero coefficients of an algebraic power series over a field of characteristic $p > 0$ is p-automatic. It thus seems reasonable to conjecture that if $f(n)$ is a holonomic sequence taking integer values and p is a prime number, then the zero set of the reduction of $f(n)$ (mod p) is a p-automatic set.

The proof of Theorem 1·3 uses p-adic methods and consists of three steps. The first step uses an argument of Lech to show that one can assume the base field K is $\mathbb{Q}_p$, for some prime p, and the nonzero coefficients of the polynomials $P_i(z)$ in (1·3) are units in the p-adic integers. The next step involves showing that there exists a positive integer b such that for $c \in \{0, \ldots, b-1\}$, the sequence $f(bn+c)$ can be embedded in an 'analytic arc', in the sense that there exists a p-adic analytic map $g : \mathbb{Z}_p \to \mathbb{Z}_p$ such that $g(n) = f(bn+c)$. We then use a theorem of Strassman (see Section 2) to show that $\{n \in \mathbb{N} : f(bn+c) = 0\}$ is either finite or $\mathbb{N}$. The difficult step is the second step, in which one must find a p-adic analytic map that agrees with a subsequence on the natural numbers. In the case that $f(n)$ satisfies a linear recurrence over a field K, it is well known (see, for example, Everest, van der Poorten, Shparlinski, and Ward [**13**, section 1·1·6]) that there exist constants $\gamma_{i,j} \in \overline{K}$ and $\alpha_1, \ldots, \alpha_m \in \overline{K}$ such that, for some positive integer N and all n sufficiently large, we have

$$f(n) = \sum_{i=1}^{m} \sum_{j=0}^{N} \gamma_{i,j} n^j \alpha_i^n.$$

Lech used this fact to show that if $K = \mathbb{C}_p$ and $|\alpha_i - 1|_p < p^{-1/(p-1)}$ then the map

$$g(z) := \sum_{i=1}^{m} \sum_{j=0}^{N} \gamma_{i,j} z^j \alpha_i^z$$

will be an analytic map that converges absolutely on the closed unit ball of $\mathbb{C}_p$. Such an expression for $f(n)$ is not available when one works with holonomic sequences, and additional work is needed to obtain the embedding into a p-adic analytic arc.

2. *Preliminaries*

This section has some of the p-adic results necessary to prove Theorem 1·3. We start with an embedding theorem due to Lech [**20**]—this result can be regarded as a p-adic analogue of the Lefschetz principle.

LEMMA 2·1. *Let K_0 be a finitely generated extension of $\mathbb{Q}$ and let $\mathcal{S}$ be a finite subset of K_0. Then there exist infinitely many primes p such that K_0 embeds in $\mathbb{Q}_p$; moreover, for all but finitely many of these primes, every nonzero element of $\mathcal{S}$ is sent to a unit in $\mathbb{Z}_p$.*

Proof. The first-named author [**3**, lemma 3·1] used the Chebotarev density theorem (see Lang [**18**, theorem 10, p. 169]) to show that the set of primes p having the required property has positive density.

The other main result from p-adic analysis required is Strassman's theorem [**34**], which asserts that if a power series $f(z) \in \mathbb{Q}_p[[z]]$ converges in the closed p-adic unit disc

$$\overline{B_{\mathbb{Q}_p}(0;1)} := \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leqslant 1\} \quad (= \mathbb{Z}_p),$$

and has infinitely many zeros in this disk, then it is identically zero. A power series $f(z) \in \mathbb{Q}_p[[z]]$ that converges in the closed p-adic unit disc will be called a *rigid p-adic power series*.

To prove Theorem 1·3, we use the following ring $\mathcal{MP}_p[z]$ of polynomials.

Definition 2·2. Given a prime p, let $\mathcal{MP}_p[z]$ be the subring of the polynomial ring $\mathbb{Q}_p[z]$ consisting of the polynomials which map $\mathbb{Z}_p$ into itself.

Clearly $\mathbb{Z}_p[z] \subseteq \mathcal{MP}_p[z] \subseteq \mathbb{Q}_p[z]$. A theorem of Mahler [**25**, p. 49–50] shows that for p a prime,

$$\mathcal{MP}_p[z] = \left\{ \sum_{i=0}^{m} \alpha_i \binom{z}{i} : m \geqslant 0 \text{ and } \alpha_i \in \mathbb{Z}_p \right\}. \tag{2·4}$$

3. *Proof of Theorem* 1·3

We begin with a simple lemma.

LEMMA 3·1. *Let p be prime and suppose that $Q_1(z), \ldots, Q_d(z) \in \mathcal{MP}_p[z]$ are such that each is congruent modulo $p\mathcal{MP}_p[z]$ to a polynomial in $\mathcal{MP}_p[z]$ of degree at most N. Then there exist $H_1(z), \ldots, H_d(z) \in \mathcal{MP}_p[z]$, each of degree at most $N+1$, with $H_1(0) = \cdots = H_d(0) = 0$, such that*

$$\begin{bmatrix} H_1(z+1) \\ \vdots \\ H_d(z+1) \end{bmatrix} \equiv \begin{bmatrix} H_1(z) \\ \vdots \\ H_d(z) \end{bmatrix} - \begin{bmatrix} Q_1(z) \\ \vdots \\ Q_d(z) \end{bmatrix} \big(\text{mod } p\mathcal{MP}_p[z]\big). \tag{3·5}$$

Proof. It is no loss of generality to assume that $Q_1(z), \ldots, Q_d(z)$ each have degree at most N. Thus

$$Q_i(z) = \sum_{k=0}^{N} \alpha_{i,k} \binom{z}{k}$$

with each $\alpha_{i,k} \in \mathbb{Z}_p$. Let

$$H_i(z) := -\sum_{k=0}^{N} \alpha_{i,k} \binom{z}{k+1}. \tag{3·6}$$

Then $H_i(z) \in \mathcal{MP}_p[z]$, and it is of degree at most $N+1$. It is easy to check that this gives a solution to equation (3·5), using the identity

$$\binom{z+1}{k+1} - \binom{z}{k+1} = \binom{z}{k}.$$

Furthermore, $H_i(0) = 0$ for $1 \leqslant i \leqslant d$.

To create analytic maps for the modified version of the p-adic analytic arc lemma, we will use the following lemma about a subalgebra of $\mathcal{MP}_p[z]$.

LEMMA 3·2. *Given a prime p and a positive integer m, let*

$$S_m := \left\{ \gamma + \sum_{i=1}^{m} p^i H_i(z) \;\middle|\; \gamma \in \mathbb{Z}_p,\ H_i(z) \in \mathcal{MP}_p[z],\ \deg\big(H_i(z)\big) \leqslant 2i-1 \right\}$$

and

$$T_m := S_m + \left\{ \gamma + \sum_{i=1}^{n} p^i H_i(z) \;\middle|\; n \geqslant 1,\ \gamma \in \mathbb{Z}_p,\ H_i(z) \in \mathcal{MP}_p[z],\ \deg\big(H_i(z)\big) \leqslant 2i-2 \right\}.$$

Then T_m is a $\mathbb{Z}_p$-subalgebra of $\mathcal{MP}_p[z]$. Moreover, if $\alpha \in p\mathbb{Z}_p$ and $\beta \in \mathbb{Z}_p$, then for any polynomial $P(z) \in \mathbb{Z}_p[z]$, one has $P(\beta + \alpha z) \in T_m$, for $m \geqslant 1$. In particular, $\mathbb{Z}_p[pz] \subseteq T_m$ for $m \geqslant 1$.

Proof. Since T_m is closed under addition and multiplication by p-adic integers, to show T_m is a $\mathbb{Z}_p$-algebra, it is sufficient to show that T_m is closed under multiplication. Since T_m is contained in the $\mathbb{Z}_p$-span of the constant function 1 and elements of the form $p^i H(z)$ for some $i \geqslant 1$ and $H(z) \in \mathcal{MP}_p[z]$ a polynomial of degree at most $2i-1$, it suffices to check that if i and j are positive integers and $H(z), G(z) \in \mathcal{MP}_p[z]$ are polynomials of degrees at most $2i-1$ and $2j-1$ respectively, then the product $p^i H(z) \cdot p^j G(z)$ lies in T_m. Note that this follows since $H(z)G(z) \in \mathcal{MP}_p[z]$ has degree at most $2(i+j)-2$ and so the product is of the form $p^{i+j} L(z)$ for some $L(z) \in \mathcal{MP}_p[z]$ of degree at most $2(i+j)-2$.

Next suppose $m \geqslant 1, \alpha \in p\mathbb{Z}_p$, $\beta \in \mathbb{Z}_p$, and $P(z) \in \mathbb{Z}_p[z]$. Then α in $p\mathbb{Z}_p$ implies $\beta + \alpha z \in T_m$; and since T_m is a $\mathbb{Z}_p$-algebra, it follows that $P(\beta + \alpha z) \in T_m$, and so, in particular, $\mathbb{Z}_p[pz] \subseteq T_m$.

Given a positive integer d and a ring R with identity element, we let $\mathsf{M}_d(R)$ denote the set of $d \times d$ matrices with entries from R. When working with a matrix ring $\mathsf{M}_d(R)$, we take $\mathbf{I}$ to be the $d \times d$ identity matrix.

LEMMA 3·3 (Analytic arc lemma). *Let d be a natural number, let $p \geqslant 5$ be prime, let $\mathbf{v} = [v_1 \cdots v_d]^T \in \mathbb{Z}_p^d$, and let $\mathbf{A}(z) := \big(a_{ij}(z)\big) \in \mathsf{M}_d\big(\mathbb{Z}_p[pz]\big)$ with $\mathbf{A}(0) \equiv \mathbf{I} \pmod{p\mathsf{M}_d\big(\mathbb{Z}_p\big)}$. Then there exist rigid p-adic power series $f_1(z), \ldots, f_d(z)$ such that $f_i(0) = v_i$ for $i \in \{1, \ldots, d\}$ and*

$$\begin{bmatrix} f_1(z+1) \\ \vdots \\ f_d(z+1) \end{bmatrix} = \mathbf{A}(z) \cdot \begin{bmatrix} f_1(z) \\ \vdots \\ f_d(z) \end{bmatrix}.$$

Proof. Let S_m and T_m be as in the statement of Lemma 3·2. The desired tuple $\big(f_1(z), \ldots, f_d(z)\big)$ of power series will be successively approximated by tuples of polynomials $\big(G_{1,j}(z), \ldots, G_{d,j}(z)\big)$, that is, $f_i(z) - G_{i,j}(z) \in p^j \mathcal{MP}_p[z]$, for $1 \leqslant i \leqslant d$ and $j \geqslant 0$. Let

$$G_{i,0}(z) := v_i \quad \text{for } 1 \leqslant i \leqslant d.$$

It will be proved, by induction on m, that one can recursively find $H_{i,m}(z) \in \mathcal{MP}_p[z]$, for $1 \leqslant i \leqslant d$, such that by setting

$$G_{i,m}(z) := v_i + \sum_{k=1}^{m} p^k H_{i,k}(z), \tag{3·7}$$

one has the following three conditions holding:

(i) $H_{i,m}(0) = 0$ for $1 \leqslant i \leqslant d$;
(ii) $H_{i,m}(z) \in S_m$, for $1 \leqslant i \leqslant d$; and
(iii) $G_{i,m}(z+1) - \sum_{j=1}^{d} a_{i,j}(z) G_{j,m}(z) \in p^{m+1}\mathcal{MP}_p[z]$.

The base case of the induction is $m = 0$. In this case, conditions (i) and (ii) are vacuous, and (iii) holds since $\mathbf{A}(z)$ is congruent modulo p to the identity matrix.

Let $m \geqslant 0$ and assume that the $H_{i,k}(z)$ have been found, for $1 \leqslant i \leqslant d$ and $0 \leqslant k \leqslant m$, such that conditions (i)–(iii) hold for $0 \leqslant k \leqslant m$. The method is to find polynomials $H_{i,m+1}(z) \in \mathcal{MP}_p[z]$ such that, with $G_{i,m+1}(z)$ defined as in (3·7), conditions (i)–(iii) hold.

By (iii), there are polynomials $Q_{i,m}(z) \in \mathcal{MP}_p[z]$, for $1 \leqslant i \leqslant d$, such that

$$p^{m+1} Q_{i,m}(z) = G_{i,m}(z+1) - \sum_{j=1}^{d} a_{i,j}(z) G_{j,m}(z). \tag{3·8}$$

Then Definition (3·7) and condition (ii) show that $G_{1,m}(z), \ldots, G_{d,m}(z)$ as well as

$$G_{1,m}(z+1), \ldots, G_{d,m}(z+1)$$

are in S_m. Thus, by Lemma 3·2 and the fact that the $a_{ij}(z)$ are in $\mathbb{Z}_p[pz]$, $p^{m+1} Q_{i,m}(z)$ is in the $\mathbb{Z}_p$-algebra T_m. It follows that

$$p^{m+1} Q_{i,m}(z) = \gamma_{i,m} + \sum_{k=1}^{n} p^k Q_{i,m,k}(z)$$

for some $\gamma_{i,m} \in \mathbb{Z}_p$, and for some polynomials $Q_{i,m,k}(z) \in \mathcal{MP}_p[z]$ such that $\deg(Q_{i,m,k}(z)) \leqslant 2k-1$ for $k \leqslant m$ and $\deg(Q_{i,m,k}(z)) \leqslant 2k-2$ for $k > m$.

Consequently, $p^{m+1} Q_{i,m}(z)$ is equivalent modulo $p^{m+2}\mathcal{MP}_p[z]$ to the polynomial

$$\gamma_{i,m} + \sum_{k=1}^{m+1} p^k Q_{i,m,k}(z),$$

a polynomial in $\mathcal{MP}_p[z]$ of degree at most $2m$. Hence $Q_{i,m}(z)$ is congruent modulo $p\mathcal{MP}_p[z]$ to a polynomial in $\mathcal{MP}_p[z]$ of degree at most $2m$.

Note that the definition (3·7) of $G_{i,m+1}(z)$ can be replaced by

$$G_{i,m+1}(z) := G_{i,m}(z) + p^{m+1} H_{i,m+1}(z).$$

To satisfy property (iii), it is sufficient to find $H_{i,m+1}(z) \in \mathcal{MP}_p[z]$, $1 \leqslant i \leqslant d$, such that

$$G_{i,m}(z+1) + p^{m+1} H_{i,m+1}(z+1) - \sum_{j=1}^{d} a_{i,j}(z)\big(G_{j,m}(z) + p^{m+1} H_{j,m+1}(z)\big)$$

is in $p^{m+2}\mathcal{MP}_p[z]$, for $i \in \{1, \ldots, d\}$. This expression is congruent modulo $p^{m+2}\mathcal{MP}_p[z]$ to

$$p^{m+1} Q_{i,m}(z) + p^{m+1} H_{i,m+1}(z+1) - p^{m+1} \sum_{j=1}^{d} a_{i,j}(z) H_{j,m+1}(z).$$

However, since each $a_{i,j}(z) \in \delta_{i,j} + p\mathcal{MP}_p[z]$, we see that this simplifies as

$$p^{m+1} Q_{i,m}(z) + p^{m+1} H_{i,m+1}(z+1) - p^{m+1} H_{i,m+1}(z)$$

modulo $p^{m+2}\mathcal{MP}_p[z]$. It therefore suffices to solve the system

$$Q_{i,m}(z) + H_{i,m+1}(z+1) - H_{i,m+1}(z) \equiv 0 \pmod{p\mathcal{MP}_p[z]}, \tag{3·9}$$

for $i \in \{1, \ldots, d\}$, where each $Q_{i,m}$ is congruent modulo $p\mathcal{MP}_p[z]$ to a polynomial of degree at most $2m$.

The hypotheses of the statement of Lemma 3·1 are satisfied by the system (3·9), so we conclude that there exists a solution $[H_{1,m+1}(z), \ldots, H_{d,m+1}(z)] \in \mathcal{MP}_p[z]^d$ with $H_{i,m+1}(0) = 0$ for $1 \leqslant i \leqslant d$ and with $H_{i,m+1}(z)$ of degree at most $2(m+1) - 1$. Thus conditions (i)–(iii) are satisfied, completing the induction step.

We set

$$f_i(z) := v_i + \sum_{j=1}^{\infty} p^j H_{i,j}(z).$$

Then each $H_{i,j}(z) \in \mathcal{MP}_p[z]$ is of degree at most $2j-1$ and hence

$$H_{i,j}(z) = \sum_{k=0}^{2j-1} \gamma_{i,j,k} \binom{z}{k},$$

with $\gamma_{i,j,k} \in \mathbb{Z}_p$. (Let $\gamma_{i,j,k} = 0$ for $k > 2j-1$.) We find that

$$\begin{aligned} f_i(z) &= v_i + \sum_{j=1}^{\infty} p^j \left(\sum_{k=0}^{2j-1} \gamma_{i,j,k} \binom{z}{k} \right) \\ &= v_i + \sum_{k=0}^{\infty} \beta_{i,k} \binom{z}{k}, \end{aligned} \tag{3·10}$$

in which

$$\beta_{i,k} := \sum_{j=1}^{\infty} p^j \gamma_{i,j,k}$$

is absolutely convergent p-adically, since each $\gamma_{i,j,k} \in \mathbb{Z}_p$. To show that the series (3·10) defines an analytic function on $\mathbb{Z}_p$, we must establish that $|\beta_{i,k}|_p/|k!|_p \to 0$ as $k \to \infty$ (see Robert [**30**, theorem 4·7, p. 354]); that is, for any $j > 0$ one has $\beta_{i,k}/k! \in p^j\mathbb{Z}_p$ for all sufficiently large k. To do this, we note that $\gamma_{i,j,k} = 0$ if $j < (k+1)/2$. Hence

$$\beta_{i,k} = \sum_{j \geqslant (k+1)/2} p^j \gamma_{i,j,k}.$$

It follows that $|\beta_{i,k}|_p \leqslant p^{-(k+1)/2}$. Since $1/|k!|_p < p^{k/(p-1)}$, we see that $\beta_{i,k}/k! \to 0$ since $p > 3$. Hence $f_1, \ldots, f_d$ are rigid analytic maps on $\mathbb{Z}_p$.

Finally, observe that the argument above showed that

$$f_i(z) \equiv G_{i,j}(z) \pmod{p^j\mathcal{MP}_p[z]}.$$

It then follows from property (iii) above that

$$f_i(z+1) \equiv \sum_{\ell=1}^{d} a_{i,\ell}(z) f_\ell(z) \pmod{p^j\mathcal{MP}_p[z]}$$

for $i \in \{1, \ldots, d\}$.

Since this holds for all $j \geqslant 1$, we conclude that

$$\begin{bmatrix} f_1(z+1) \\ \vdots \\ f_d(z+1) \end{bmatrix} = \mathbf{A}(z) \cdot \begin{bmatrix} f_1(z) \\ \vdots \\ f_d(z) \end{bmatrix}.$$

Finally, we have

$$f_i(0) = v_i + \sum_{j=1}^{\infty} p^j H_{i,j}(0) = v_i,$$

which concludes the proof.

We are almost ready to prove our main result. The one remaining thing we need is to show how the analytic arc lemma applies to our situation. We accomplish this with the following lemma.

LEMMA 3·4. *Let p be a prime number, let d be a natural number, and let $P_1(z), \ldots, P_d(z) \in \mathbb{Z}_p[z]$. Suppose that $f : \mathbb{N} \to \mathbb{Z}_p$ is a sequence satisfying the polynomial-linear recurrence*

$$f(n) = \sum_{i=1}^{d} P_i(n) f(n-i)$$

for $n \geqslant d$. Let

$$\mathbf{B}(z) := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ P_d(z-1+d) & P_{d-1}(z-1+d) & \cdots & P_2(z-1+d) & P_1(z-1+d) \end{pmatrix},$$

and let $\mathbf{v}_0 := [f(0), \ldots, f(d-1)]^T$. Then

$$\begin{bmatrix} f(n) \\ \vdots \\ f(n+d-1) \end{bmatrix} = \mathbf{B}(n)\mathbf{B}(n-1)\cdots\mathbf{B}(1)\mathbf{v}_0,$$

for every positive integer n. Furthermore, if $P_d(z)$ is a constant that is a unit in $\mathbb{Z}_p$ then the determinant of $\mathbf{B}(z)$ is a constant that is a unit in $\mathbb{Z}_p$.

Proof. For each positive integer n let

$$\mathbf{v}_n := \begin{bmatrix} f(n) \\ \vdots \\ f(n+d-1) \end{bmatrix}.$$

Then

$$\mathbf{v}_n = \mathbf{B}(n)\mathbf{v}_{n-1},$$

for $n \geqslant 1$, leads to

$$\mathbf{v}_n = \mathbf{B}(n)\mathbf{B}(n-1)\cdots\mathbf{B}(1)\mathbf{v}_0.$$

The determinant of $\mathbf{B}(z)$ is $P_d(z-1+d)$; hence if $P_d(z)=\alpha$, a unit in $\mathbb{Z}_p$, then $\det(\mathbf{B}(z))$ equals that unit.

Proof of Theorem 1·3. It is no loss of generality to assume that the recurrence in the statement of Theorem 1·3 holds for all $n \geqslant d$. Let $\mathcal{S}$ denote the finite subset of K consisting of the nonzero $f(n)$, where $0 \leqslant n < d$, along with all nonzero coefficients of the polynomials $P_1(z), \ldots, P_d(z)$. Then we let $K_0 = \mathbb{Q}(\mathcal{S})$, the subfield of K generated by the elements of $\mathcal{S}$. By Lemma 2·1, there exists a prime $p \geqslant 5$ and a field embedding of K_0 into $\mathbb{Q}_p$ such that the image of $\mathcal{S}$ is contained in the units of $\mathbb{Z}_p$. By identifying K_0 with its image in $\mathbb{Q}_p$, we see that there is no loss of generality in assuming that $P_1(z), \ldots, P_d(z) \in \mathbb{Z}_p[z]$, with the nonzero coefficients of the $P_i(z)$ being units of $\mathbb{Z}_p$; in particular, $P_d(z)$ is a unit in $\mathbb{Z}_p$. Furthermore, after this identification, a simple induction shows that $f : \mathbb{N} \to \mathbb{Z}_p$.

Letting $\mathbf{B}(z)$ and $\mathbf{v}_0$ be as defined in the statement of Lemma 3·4, one has, for $n \geqslant d$,

$$\begin{bmatrix} f(n) \\ \vdots \\ f(n+d-1) \end{bmatrix} = \mathbf{B}(n)\mathbf{B}(n-1)\cdots\mathbf{B}(1)\mathbf{v}_0, \tag{3·11}$$

and the determinant of $\mathbf{B}(z)$ is a unit in $\mathbb{Z}_p$. In addition, observe that $(z+p)^i - z^i \in p\mathbb{Z}_p[z]$ for all nonnegative integers i and hence, by linearity, we have that $Q(z+p)-Q(z) \in p\mathbb{Z}_p[z]$ for all $Q(z) \in \mathbb{Z}_p[z]$. Thus we have $\mathbf{B}(z+p) - \mathbf{B}(z) \in p\mathsf{M}_d\big(\mathbb{Z}_p[z]\big)$, since the entries of $\mathbf{B}(z)$ are in $\mathbb{Z}_p[z]$.

Let $\varphi : M_d(\mathbb{Z}_p) \to M_d(\mathbb{Z}/p\mathbb{Z})$ be the canonical surjection. For $n \in \mathbb{Z}$, $\mathbf{B}(n) \in \mathsf{M}_d(\mathbb{Z}_p)$, and thus $\varphi\big(\mathbf{B}(n)\big) \in \mathsf{M}_d(\mathbb{Z}/p\mathbb{Z})$. Since $\mathsf{M}_d(\mathbb{Z}/p\mathbb{Z})$ is a finite ring, there exist natural numbers m_0 and m_1 with $m_0 < m_1$ such that

$$\varphi(\mathbf{B}(pm_1)\cdots\mathbf{B}(1)) = \varphi(\mathbf{B}(pm_0)\cdots\mathbf{B}(1)).$$

Since the determinant of $\mathbf{B}(z)$ is a unit of $\mathbb{Z}_p$, the determinant of $\varphi(\mathbf{B}(i))$ is nonzero, for $i \in \mathbb{Z}$. Thus $\varphi(\mathbf{B}(i))$ is in $\mathrm{GL}_d(\mathbb{Z}/p\mathbb{Z})$ and hence $\varphi(\mathbf{B}(pm_1)\cdots\mathbf{B}(pm_0+1))$ is the identity. Furthermore, since $\varphi(\mathbf{B}(n+p)) = \varphi(\mathbf{B}(n))$ for $n \in \mathbb{Z}$, it follows that for $i \in \mathbb{Z}$, $\varphi(\mathbf{B}(pm_1+i)\cdots\mathbf{B}(pm_0+1+i))$ is similar to $\varphi(\mathbf{B}(pm_1)\cdots\mathbf{B}(pm_0+1))$ and hence

$$\varphi(\mathbf{B}(pm_1+i)\cdots\mathbf{B}(pm_0+1+i)) = \mathbf{I}. \tag{3·12}$$

Let

$$b := p(m_1-m_0).$$

Suppose that $c \in \{0, \ldots, b-1\}$. Then Equation (3·12) gives

$$\varphi(\mathbf{B}(c+b(n+1))\cdots\mathbf{B}(c+bn+1)) = \mathbf{I}, \tag{3·13}$$

for $n \in \mathbb{Z}$. Define the matrix $\mathbf{A}(z) \in \mathsf{M}_d(\mathbb{Z}_p[z])$ by

$$\mathbf{A}(z) := \mathbf{B}(c+bz)\mathbf{B}(c+bz-1)\cdots\mathbf{B}(c+bz-b+1).$$

Since p divides a, we see that for each integer i, the matrix-valued function $\mathbf{B}(i+bz) \in \mathsf{M}_d(\mathbb{Z}_p[pz])$ and hence $\mathbf{A}(z) \in \mathsf{M}_d(\mathbb{Z}_p[pz])$. Moreover, Equation (3·13) shows that for $n \in \mathbb{Z}$ we have $\varphi(\mathbf{A}(n)) = \mathbf{I}$ and in particular $\mathbf{A}(0) \equiv \mathbf{I} \pmod{p\mathsf{M}_d(\mathbb{Z}_p)}$. Let

$$\mathbf{v} := \mathbf{B}(c)\mathbf{B}(c-1)\cdots\mathbf{B}(1)\mathbf{v}_0.$$

Then from (3·11), for $n \geqslant 1$,

$$\begin{bmatrix} f(c+bn) \\ \vdots \\ f(c+bn+d-1) \end{bmatrix} = \mathbf{A}(n)\mathbf{A}(n-1)\cdots\mathbf{A}(1)\mathbf{v}.$$

Since the hypotheses in the statement of Lemma 3·3 are satisfied by $\mathbf{A}(z)$ and $\mathbf{v}$, we also have that there exist rigid p-adic power series $f_1(z), \ldots, f_d(z)$ such that, for $n \geqslant 1$,

$$\begin{bmatrix} f_1(n) \\ \vdots \\ f_d(n) \end{bmatrix} = \mathbf{A}(n)\mathbf{A}(n-1)\cdots\mathbf{A}(1)\mathbf{v}.$$

Thus for $n \geqslant 1$,

$$f_1(n) = f(c+bn).$$

By Strassman's theorem,

$$\{n \in \mathbb{N} : f_1(n) = 0\}$$

is either finite or equal to $\mathbb{N}$. Hence

$$\{n \in \mathbb{N} : f(c+bn) = 0\}$$

is either finite or equal to $\mathbb{N}$. Let

$$X := \{c \in \{0, \ldots, b-1\} : f(c+bn) = 0 \text{ for } n \in \mathbb{N}\}.$$

Then

$$\{n \in \mathbb{N} : f(n) = 0\} = Z_0 \cup \bigcup_{c \in X} (b\mathbb{N} + c),$$

where Z_0 is a finite set consisting of all n such that $f(n) = 0$ and $n \equiv c' \pmod{b}$ for some $c' \in \{0, \ldots, b-1\} \setminus X$. The result follows.

4. *Concluding remarks and examples*

We make some general remarks about Theorem 1·3 in this section.

There are some difficulties that arise with trying to extend this argument to the collection of all holonomic sequences. For example, if we take

$$f(n) = \binom{2n}{n},$$

then $f(n)$ is holonomic as it satisfies the polynomial linear recurrence

$$(n+1)f(n+1) - 2(2n+1)f(n) = 0$$

for $n \geqslant 0$. Observe that there is no way to select a prime $p \geqslant 5$ and a natural number b such that for all $c \in \{0, \ldots, b-1\}$ we have a p-adic rigid analytic map $G_c(z)$ such that $G_c(n) = f(bn+c)$ for all $n \in \mathbb{N}$. To see this, suppose that we have such a prime p and a natural number b and let $c = 0$ and let $g(z)$ be a p-adic rigid analytic map with $g(n) = f(bn)$. Since g is continuous, there is some $j \geqslant 1$ such that $|g(z+p^j) - g(z)|_p < 1/p$ for $z \in \mathbb{Z}_p$. This then gives that

$$f(bp^j k) \equiv f(0) = 1 \pmod{p}$$

for all natural numbers k. But $f(pk) \equiv f(k) \pmod{p}$ for all natural numbers k and thus we must have

$$f(bk) \equiv 1 \pmod{p}$$

for all natural numbers k. But if we choose ℓ such that $p^\ell \leqslant b < p^{\ell+1}$ and choose k to be the smallest natural number such that $2bk > p^{\ell+1}$ then we see that p divides $f(bk)$ using the formula

$$\left|\binom{2n}{n}\right|_p = p^{\sum_{j\geqslant 1} 2\lfloor n/p^j\rfloor - \lfloor 2n/p^j\rfloor},$$

and noting that each term appearing in the sum on the right-hand side is non-positive and that the term is strictly negative when $j = \ell + 1$. This is a contradiction.

In an earlier paper, the authors [**5**] considered the set of zero coefficients to functions arising from solutions to a system of equations with certain prescribed properties. In many cases, the solution sets were algebraic functions and hence differentiably finite. The hypotheses guaranteed that the zero set was a finite union of arithmetic progressions along with a finite set, although the methods used were very different and relied on studying the behaviour of power series defined by systems of equations.

We also observe that $f(n)$ is a holonomic $\mathbb{Z}$-valued sequence that satisfies a polynomial-linear recurrence of the form

$$f(n) = \sum_{i=1}^{d} P_i(n) f(n-i),$$

then the argument we employed to prove that the zero set of $f(n)$ is a finite union of infinite arithmetic progressions along with a finite set can be proved under more general conditions. In particular, it is sufficient that there exist infinitely many primes p for which $P_d(x)$ does not have any roots modulo p. The Chebotarev density theorem (see Lang [**18**, theorem 10, p. 169]) gives that this will occur precisely when there is some automorphism of the splitting field of $P_d(x)$ over $\mathbb{Q}$ whose natural action on the roots of $P_d(x)$ does not have any fixed points.

Finally, we note that Theorem 1·3 is ineffective in the sense that if we know that our recurrence has only finitely many zeros, we cannot effectively bound the size of the largest zero in terms of data coming from the recurrence and the initial terms of the recurrence. Indeed, this is a notoriously difficult problem for linear recurrences and much work has been done on this problem by Evertse, Schlickewei, and Schmidt [**14**], who showed how one can obtain a quantitative version of the Skolem-Mahler-Lech theorem that bounds the number of exceptional zeros and the lengths of the arithmetic progressions in terms of such data.

REFERENCES

[**1**] B. ADAMCZEWSKI and J. P. BELL. On the set of zero coefficients of algebraic power series. *Invent. Math.* **187**, no. 2 (2012), 343–393.

[**2**] J.-P. ALLOUCHE and J. SHALLIT. *Automatic Sequences. Theory, Applications, Generalizations* (Cambridge University Press, 2003).

[**3**] J. P. BELL. A generalised Skolem–Mahler–Lech Theorem for affine varieties. *J. London Math. Soc.* 73 (2006), 367–379.

[**4**] J. P. BELL. Corrigendum to "A generalised Skolem–Mahler–Lech Theorem for affine varieties". *J. London Math. Soc.* 78 (2008), 267–272.

[**5**] J. P. BELL, S. N. BURRIS and K. YEATS. *Spectra and Systems of Equations.* `arXiv:0911.2494`.

[**6**] J. P. BELL, D. GHIOCA and T. J. TUCKER. The dynamical Mordell–Lang problem for étale maps. *Amer. J. Math.* **132**, no. 6 (2010), 1655–1675.
[**7**] J.-P. BÉZIVIN. Une généralisation du théorème de Skolem–Mahler–Lech. *Quart. J. Math. Oxford Ser.* (2). **40** (1989), no. 158, 133–138.
[**8**] J.-P. BÉZIVIN and V. LAOHAKOSOL. On the theorem of Skolem–Mahler–Lech. *Exposition. Math.* **9** (1991), no. 1, 89–96.
[**9**] M. BOUSQUET–MÉLOU. Walks in the quarter plane: Kreweras' algebraic model. *Ann. Appl. Probab.* **15** (2005), no. 2, 1451–1491.
[**10**] F. CHYZAK and B. SALVY. Non-commutative elimination in Ore algebras proves multivariate identities. *J. Symbolic Comput.* **26** (1998), no. 2, 187–227.
[**11**] F. CHYZAK, M. MISHNA and B. SALVY, BRUNO. Effective scalar products of D-finite symmetric functions. *J. Combin. Theory Ser. A* **112** (2005), no. 1, 1–43.
[**12**] H. DERKSEN. A Skolem–Mahler–Lech theorem in positive characteristic and finite automata. *Invent. Math.* **168** (2007), 175–224.
[**13**] G. EVEREST, A. VAN DER POORTEN, ALF, I. SHPARLINSKI and T. WARD. *Recurrence sequences*. Mathematical Surveys and Monographs, 104 (*Amer. Math. Soc.* 2003).
[**14**] J.–H. EVERTSE, H. P. SCHLICKEWEI and W. M. SCHMIDT. Linear equations in variables which lie in a multiplicative group. *Ann. of Math.* (2) **155** (2002), no. 3, 807–836.
[**15**] S. GAROUFALIDIS. G-functions and multisum versus holonomic sequences. *Adv. Math.* **220** (2009), no. 6, 19451955.
[**16**] I. GESSEL. Symmetric functions and P-recursiveness. *J. Combin. Theory Ser. A* **53** (1990), no. 2, 257–285.
[**17**] G. HANSEL. Une démonstration simple du théorème de Skolem–Mahler–Lech. *Theoret. Comput. Sci.* **43** (1986), no. 1, 91–98.
[**18**] S. LANG. *Algebraic number theory. Second edition.* Graduate Texts in Mathematics, 110 (Springer-Verlag, 1994).
[**19**] V. LAOHAKOSOL. Some extensions of the Skolem–Mahler–Lech theorem. *Exposition. Math.* **7** (1989), no. 2, 137–187.
[**20**] C. LECH. A note on recurring series. *Ark. Mat.* **2** (1953), 417–421.
[**21**] H. LI and F. VAN OYSTAEYEN. Elimination of variables in linear solvable polynomial algebras and ∂-holonomicity. *J. Algebra* **234** (2000), no. 1, 101–127.
[**22**] K. MAHLER. Eine arithmetische Eigenshaft der Taylor–Koeffizienten rationaler Funktionen. *Proc. Kon. Nederlandsche Akad. v. Wetenschappen* **38** (1935), 50–60.
[**23**] K. MAHLER. On the Taylor coefficients of rational functions. *Proc. Camb. Phil. Soc.* **52** (1956), 39–48.
[**24**] K. MAHLER. Addendum to the paper "On the Taylor coefficients of rational functions". *Proc. Camb. Phil. Soc.* **53** (1957), 544.
[**25**] K. MAHLER. *p-adic Numbers and Their Functions, Second ed.* (Cambridge University Press, Cambridge, New York, 1981).
[**26**] C. METHFESSEL. On the zeros of recurrence sequences with non-constant coefficients. *Arch. Math.* (Basel) **74** (2000), no. 3, 201–206.
[**27**] A. J. VAN DER POORTEN. A proof that Euler missed ... Apéry's proof of the irrationality of $\zeta(3)$. *Math. Intelligencer* **1** (1979), 195–203.
[**28**] A. J. VAN DER POORTEN. Some facts that should be better known; especially about rational functions. *Number Theory and Applications* ed. Richard A. Mollin, (NATO–Advanced Study Institute, Banff, 1988), (Kluwer Academic Publishers, 1989), 497–528.
[**29**] A. J. VAN DER POORTEN and R. TIJDEMAN. On common zeros of exponential polynomials. *Enseign. Math.* (2) **21** (1975), no. 1, 57–67.
[**30**] A. ROBERT. *A course in p-adic analysis.* Graduate Texts in Mathematics, 198 (Springer-Verlag, 2000).
[**31**] L. A. RUBEL. Some research problems about algebraic differential equations. *Trans. Amer. Math. Soc.* **280** (1983), no. 1, 43–52 (Problem 16).
[**32**] T. SKOLEM. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen. *C. r. 8 Congr. Scand. à Stockholm* (1934), 163–188.
[**33**] R. Stanley, Differentiably finite power series. *European J. Combin.* **1** (1980), 175–188.
[**34**] R. STRASSMAN. Über den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen. *J. Reine Angew. Math.* **159** (1928), 13–28; 65–66.
[**35**] H. S. WILF and D. ZEILBERGER. An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities. *Invent. Math.* **108** (1992), no. 3, 575–633.