Available online at www.sciencedirect.com
SCIENCE DIRECT
Advances in Applied Mathematics 34 (2005) 634–643
ADVANCES IN Applied Mathematics
www.elsevier.com/locate/yaama

On the values attained by a k-regular sequence

Jason P. Bell

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1109, USA

Received 6 October 2004; accepted 22 November 2004
Available online 22 January 2005

Abstract

A sequence is said to be k-*automatic* if the nth term of this sequence is generated by a finite state machine with n in base k as input. Allouche and Shallit first defined k-regular sequences as a natural generalization of k-automatic sequences. We study the set of values attained by a k-regular sequence and characterize sets with the property that any k-regular sequence taking values in this set is necessarily k-automatic. In particular, we show that an unbounded regular sequence must have infinitely many composite values, answering a question of Allouche and Shallit.

Keywords: k-Automatic sequences; k-Regular sequences; Rational sequences; Primes

1. Introduction

A sequence is said to be k-*automatic* if the nth term of this sequence is generated by a finite state machine with n in base k as input. The ubiquity of these sequences has been observed by several authors [2,4–6]. Another way of defining the k-automatic property comes from looking at the k-*kernel* of a sequence. The k-kernel of a sequence $\{f(n)\}_{n=0}^{\infty}$ is defined to be the collection of sequences of the form $\{f(k^i n + j)\}_{n=0}^{\infty}$ where $i \geqslant 0$ and $0 \leqslant j < k^i$. A sequence is k-automatic if and only if its k-kernel is finite. Using this definition of k-automatic sequences, Allouche and Shallit [1,2] generalized the notion of being k-automatic.

E-mail address: belljp@umich.edu.

0196-8858/$ – see front matter
doi:10.1016/j.aam.2004.11.004

Given a sequence $\{f(n)\}_{n=0}^{\infty}$ taking values in some abelian group, we create a $\mathbb{Z}$-module $M(\{f(n)\}; k)$ which is defined to be the $\mathbb{Z}$-module generated by all sequences $\{f(k^i n + j)\}_{n=0}^{\infty}$, where $i \geqslant 0$ and $0 \leqslant j < k^i$.

Definition 1. A sequence is *k-regular* if $M(\{f(n)\}; k)$ is finitely generated as a $\mathbb{Z}$-module.

Since the k-kernel of a sequence $\{f(n)\}$ spans $M(\{f(n)\}; k)$ as a $\mathbb{Z}$-module, we see that a k-automatic sequence is necessarily k-regular.

We look at k-regular sequences taking on integer values. In this case, the $\mathbb{Z}$-module $M(\{f(n)\}; k)$ is torsion free and hence isomorphic to a finite direct sum of copies of $\mathbb{Z}$. We investigate the set of values that can be attained by such sequences. We characterize the sets S such that any k-regular sequence which takes all its values in S is necessarily k-automatic.

The property that is really important in answering this question is the *finite orbit property*. Given a subset S of the integers, we let S^d denote all $d \times 1$ column vectors whose coordinates are all in S.

Definition 2. We say that a subset S of $\mathbb{Z}$ has the *finite orbit property* if whenever there exist

- a set $T \subseteq S^d$ with the property that the $\mathbb{Q}$-span of the vectors in T is $\mathbb{Q}^d$;
- a $d \times d$ invertible matrix A with entries in $\mathbb{Q}$ such that $AT \subseteq T$,

the matrix A necessarily satisfies $A^m = I$ for some m.

Our main result is the following.

Theorem 3. *Let S be a subset of the integers. Then the following are equivalent*:

- *S has the finite orbit property*;
- *any rational power series whose coefficients all lie in S has the property that its sequence of coefficients is eventually periodic*;
- *any k-regular sequence whose values all lie in S is k-automatic.*

We also give examples of sets with the finite orbit property; for example, the set of prime numbers has this property. This answers a question of Allouche and Shallit [2], as it follows that a k-regular sequence with unbounded values must have infinitely many occurrences of composite numbers.

2. The finite orbit property

Here we study the finite orbit property and give some equivalent properties. We use the finite orbit property as a base case in an induction argument to prove our key result.

Proposition 4. *Let S be a set with the finite orbit property and let*

$$T := \{\mathbf{v}(n)\} \subseteq S^d \subseteq \mathbb{Q}^d$$

be a sequence of vectors which span $\mathbb{Q}^d$. Suppose there is a finite set $\mathcal{U}$ of $d \times d$ matrices such that $AT \subseteq T$ for all $A \in \mathcal{U}$. Then the monoid generated by the matrices in $\mathcal{U}$ is finite.

Proof. We prove this using a double induction. First suppose that $d = 1$. Then we can regard $\mathcal{U}$ as a finite set of rational numbers. If the rational numbers are all 0, then the monoid generated by $\mathcal{U}$ is just $\{0, 1\}$. If $a \neq 0$ is a nonzero element of $\mathcal{U}$, then $aT \subseteq T$. Since S has the finite orbit property, we see that $a^m = 1$ for some m. Hence $a = \pm 1$, since a is a rational number. Thus $\mathcal{U} \subseteq \{0, \pm 1\}$ and the result follows in this case. Now suppose that the claim is true whenever $d < e$ and consider the case that $d = e$.

Let $\mathcal{U}$ be matrices satisfying the condition given in the statement of the proposition. We now use induction on the size of $\mathcal{U}$.

If the size of $\mathcal{U} = 0$ then the submonoid of the $e \times e$ matrices generated by $\mathcal{U}$ is just the identity matrix, which is a finite set. Now suppose that the claim is true whenever $\mathcal{U}$ has fewer than m elements and consider the case that $\mathcal{U}$ has size m. Write $\mathcal{U} = \{A_1, \ldots, A_m\}$ and let $\mathcal{X}$ denote the monoid generated by $A_1, \ldots, A_m$. We have two cases.

Case I. The matrices in $\mathcal{U}$ are all invertible.

Notice that any matrix B in $\mathcal{X}$ has the property that $BT \subseteq T$. Since B is invertible and S has the finite orbit property, we see that $B^m = I$. It follows that $\mathcal{X}$ is in fact a group, since the inverse of any element of $\mathcal{X}$ can be obtained by taking an appropriate power of the element. Since $\mathcal{X}$ is a finitely generated torsion subgroup of $\mathrm{GL}_n(\mathbb{Q})$, by the Burnside–Schur theorem (see Theorem 8.1.11 of Robinson [9]) we see that $\mathcal{X}$ is finite.

Case II. Some matrix in $\mathcal{U}$ is not invertible.

Without loss of generality A_m is not invertible. By the inductive hypothesis the submonoid $\mathcal{Y}$ of $\mathcal{X}$ generated by $A_1, \ldots, A_{m-1}$ is finite. Let $B_1, \ldots, B_p$ denote the matrices in $\mathcal{Y}$. Consider the set of matrices $A_m B_1, \ldots, A_m B_p$. Clearly $A_m B_i T \subseteq A_m T \subseteq T$ for $1 \leqslant i \leqslant p$. By assumption the vectors in T span $\mathbb{Q}^e$. Since A_m is not invertible, the span of the vectors in $A_m T$ must have dimension strictly smaller than e. Let V denote the $\mathbb{Q}$-span of the vectors in $A_m T$. Let

$$\mathbf{w}(n) = \begin{bmatrix} w_1(n) \\ \vdots \\ w_e(n) \end{bmatrix} := A_m \mathbf{v}(n).$$

Then since the span of the vectors $\{w(n)\}$ has dimension less than e, the functions $w_1(n), \ldots, w_e(n)$ are linearly dependent over $\mathbb{Q}$. Without loss of generality $w_1(n), \ldots,$

$w_{e'}(n)$ form a basis for the span of these sequences. Let $\mathbf{u}(n)$ denote the $e' \times 1$ vector whose jth coordinate is $w_j(n)$. There is an isomorphism

$$\Phi : V \to \mathbb{Q}^{e'}$$

which sends $\mathbf{w}(n)$ to $\mathbf{u}(n)$ for all $n \geqslant 0$. Since $A_m B_i (A_m T) \subseteq (A_m T)$ for $1 \leqslant i \leqslant p$, $A_m B_i$ can be regarded as a $\mathbb{Q}$-endomorphism of V for each applicable i. Thus for $1 \leqslant i \leqslant p$, we get an $e' \times e'$ matrix C_i with rational entries, defined by

$$C_i \Phi(\mathbf{v}) = \Phi(A_m B_i \mathbf{v}) \quad \text{for } \mathbf{v} \in V.$$

Since $e' < e$, we see using our inductive hypothesis that the monoid generated by $C_1, \ldots, C_p$ is finite. It follows that if we regard $A_m B_i$ as an endomorphism of V for $1 \leqslant i \leqslant p$, then the monoid generated by these endomorphisms of V is finite. Let $D_1, \ldots, D_q$ denote the distinct endomorphisms of V in the monoid generated by $\{A_m B_i \mid 1 \leqslant i \leqslant p\}$. Observe that any element of $\mathcal{X}$ can be written as

$$B_{i_0} A_m B_{i_1} A_m \cdots B_{i_{j-1}} A_m B_{i_j}$$

for some $j \geqslant 0$ and some $B_{i_0}, \ldots, B_{i_j} \in \mathcal{Y}$. Let

$$E = B_{i_0} A_m B_{i_1} A_m \cdots B_{i_{j-1}} A_m B_{i_j} \in \mathcal{X}.$$

If $j \geqslant 2$, then there exists some k with $1 \leqslant k \leqslant q$ such that for any vector $\mathbf{v} \in \mathbb{Q}^d$, we have

$$\begin{aligned} E\mathbf{v} &= B_{i_0} A_m B_{i_1} A_m B_{i_2} \cdots A_m B_{i_{j-1}} A_m B_{i_j} \mathbf{v} \\ &= B_{i_0} (A_m B_{i_1} A_m B_{i_2} \cdots A_m B_{i_{j-1}})(A_m B_{i_j} \mathbf{v}) \\ &= B_{i_0} L_k (A_m B_{i_j} \mathbf{v}) \quad (\text{since } A_m B_{i_j} \mathbf{v} \in V) \\ &= B_{i_0} L_k A_m B_{i_j} \mathbf{v}. \end{aligned}$$

Consequently, if $j \geqslant 2$ then

$$E = B_i L_k A_m B_\ell$$

for some $k \leqslant q$ and for $i, \ell \in [1, p]$. If $j = 0$, then $E = B_i$ for some $i \leqslant p$. Finally, if $j = 1$, then $E = B_i A_p B_\ell$ for some $1 \leqslant i, \ell \leqslant p$. Thus $\mathcal{X}$ is finite.

Thus we see that in either case $\mathcal{X}$ is finite and so the claim now follows by induction. □

The finite orbit property has the following interpretation in terms of rational power series.

Proposition 5. *A set S has the finite orbit property if and only if any rational power series whose coefficients all lie in S has the property that its sequence of coefficients is eventually periodic.*

Proof. Suppose that S has the finite orbit property. Let $f(z)$ be a rational power series whose coefficients all lie in S. Let $a(n)$ denote the coefficient of z^n in $f(z)$. Then we have a rational recurrence

$$a(n) = c_1 a(n-1) + \cdots + c_d a(n-d),$$

for some d and some rational numbers $c_1, \ldots, c_d$, which holds for all n sufficiently large. Choose d minimal and define

$$\mathbf{v}(n) = \begin{bmatrix} a(n) \\ \vdots \\ a(n+d-1) \end{bmatrix} \in S^d.$$

Then there is some $d \times d$ matrix A such that $A\mathbf{v}(n) = \mathbf{v}(n+1)$ for n sufficiently large. By minimality of d, A is invertible. Also, the vectors $\mathbf{v}(n)$ with n sufficiently large span $\mathbb{Q}^d$ by minimality of d. Since S has the finite orbit property we see that $A^m = I$ for some m. Consequently $\mathbf{v}(n+m) = \mathbf{v}(n)$ for all n sufficiently large. It follows that $a(n+m) = a(n)$ for all n sufficiently large and so the sequence of coefficients of $f(z)$ is eventually periodic.

Conversely, suppose that S has the property that any rational power series whose coefficients are all in S must have an eventually periodic sequence of coefficients. Let T be a set of vectors in S^d whose span is $\mathbb{Q}^d$ and suppose that A is a $d \times d$ invertible matrix with $AT \subseteq T$. Let $\mathbf{v} \in T$. Define

$$f_i(z) = \sum_{n=0}^{\infty} e_i^{\mathrm{T}} A^n \mathbf{v} z^n.$$

Then by a theorem of Schützenberger [10] (see, also, Proposition 1.1 of Hansel [7]), $f_1(z), \ldots, f_d(z)$ are all rational power series whose coefficients lie in S. Hence their sequences of coefficients are all eventually periodic. Taking the lcm of these periods, we see that $A^m\mathbf{v} = \mathbf{v}$ for some m. Since the vectors in T span $\mathbb{Q}^d$ we conclude that $A^\ell = I$ for some ℓ. Hence S has the finite orbit property. □

Proposition 6. *Let S be a set with the finite orbit property. Then $S \cup T$ has the finite orbit property for any finite set T.*

Proof. By induction it suffices to prove this when $T = \{m\}$ is a singleton. Suppose that the statement of the proposition is not true. Let $f(z) = \sum_{n \geqslant 0} f_n z^n$ be a rational power series whose coefficients lie in $S \cup \{m\}$ and which has infinitely many distinct coefficients. By the Skolem–Mahler–Lech theorem [8] the set of n such that the coefficient of z^n in $f(z)$ is equal to m is—up to a finite set—a finite union of arithmetic progressions of the form $\{an + b \mid n \geqslant 0\}$ with $a > 0$ and $0 \leqslant b < a$. Let A be the finite union of these arithmetic progressions. Then either A is the set of natural numbers, in which case we obtain the contradiction that $f(z)$ has only finitely many distinct coefficients; or, the complement of A contains an arithmetic progressions, say $\{cn + d \mid n \geqslant 0\}$. Moreover, since the complement of A is also a finite union of arithmetic progressions, it is no loss of generality to assume that the set $\{f_{cn+d} \mid n \geqslant 0\}$ is infinite. Then

$$g(z) := \sum_{n=0}^{\infty} f_{cn+d} z^n$$

is a rational function whose coefficients lie in $S \cup \{m\}$ and only finitely many of which are equal to m. Since S has the finite orbit property, we see by Proposition 5 that $g(z)$ has only finitely many distinct coefficients, a contradiction. Thus in either case we obtain a contradiction, and so we conclude that $S \cup T$ must indeed have the finite orbit property for finite sets T. □

3. Examples

We now give examples of sets with the finite orbit property.

Proposition 7. *Let S be the set of primes. Then S has the finite orbit property.*

Proof. Let T be a subset of S^d which spans all of $\mathbb{Q}^d$. Suppose that A is an invertible $d \times d$ matrix with rational entries such that $AT \subseteq T$. Let b denote the lcm of all denominators appearing in the entries of A and write $\det(A) = a/b^d$ with a a nonzero integer. Let $\mathbf{v}$ be a vector in T. Pick j such that the number of coordinates in $\mathbf{w} = A^j \mathbf{v}$ which do not divide ab is maximized. Let $p_1, \ldots, p_e$ denote the primes not dividing ab which appear as coordinates of $\mathbf{w}$. Since the entries of A do not have denominators with $p_1, \ldots, p_e$ as factors, for each i we can look at the image of A in $M_d(\mathbb{Z}/p_i\mathbb{Z})$, and this image is invertible. Thus there is some m such that $A^m \equiv I \bmod p_i$ for $1 \leqslant i \leqslant e$; that is, each entry of $A^m - I$, when written in lowest terms, has a numerator which is a multiple of $p_1 \cdots p_e$. Thus for every $\ell \geqslant 1$, $A^{m\ell}\mathbf{w}$ has the property that each of its coordinates is equivalent to the corresponding coordinates of $\mathbf{w}$ mod $p_1 \cdots p_e$. Consequently, $p_1, \ldots, p_e$ must occur in $A^{m\ell}\mathbf{w}$ in the same positions that they occur in $\mathbf{w}$. By the maximality property of $\mathbf{w}$, the remaining coordinates of $A^{m\ell}\mathbf{w}$ must divide ab. Since the number of primes dividing ab is finite, we see that there are integers n_1, n_2 with $n_1 \neq n_2$ such that $A^{mn_1}\mathbf{w} = A^{mn_2}\mathbf{w}$. Consequently, $A^{mn_1+j}\mathbf{v} = A^{mn_2+j}\mathbf{v}$. Since A is invertible, we see that there is some m' such that $A^{m'}\mathbf{v} = \mathbf{v}$. By assumption, there exist $\mathbf{v}_1, \ldots, \mathbf{v}_d$ which span $\mathbb{Q}^d$. Then for $1 \leqslant i \leqslant d$ we can find m_i such that $A^{m_i}\mathbf{v}_i = \mathbf{v}_i$. Hence $A^{m_1 \cdots m_d}$ fixes each element in our basis. It follows that $A^{m_1 \cdots m_d} = I$. The result now follows. □

Proposition 8. *Let $S = \{a_1, a_2, \ldots\}$ be a set of integers with $|a_i| \leqslant |a_{i+1}|$ for $i \geqslant 1$. Suppose that*

$$\limsup_{n \to \infty} \frac{|a_{n+1}|}{|a_n|} = \infty.$$

Then S has the finite orbit property.

Proof. Let $T \subseteq S^d$ be a set which spans $\mathbb{Q}^d$ and let A be a $d \times d$ rational matrix with the property that $AT \subseteq T$. Let $N = d\|A\|$, where $\|\cdot\|$ is the sup norm for matrices. Pick vectors $\mathbf{v}_1, \ldots, \mathbf{v}_d$ in T which form a basis for $\mathbb{Q}^d$. Pick n such that $|a_{n+1}/a_n| > N$ and for any i such that a_i is a coordinate of some $\mathbf{v}_j$, i is necessarily less than or equal to n. We claim that the coordinates of $A^m\mathbf{v}_j$ are contained in the set $\{a_1, \ldots, a_n\}$. To see this, suppose that $A^m\mathbf{v}_j$ has coordinate a_ℓ for some $\ell > n$ and some j. Pick $m \geqslant 1$ minimal and let $\mathbf{w} = A^{m-1}\mathbf{v}_j$. Then $A\mathbf{w}$ has a coordinate of the form a_ℓ with $\ell > n$ and hence

$$\|A\mathbf{w}\| \geqslant |a_{n+1}|.$$

On the other hand,

$$\|A\mathbf{w}\| \leqslant \|A\| \cdot \|\mathbf{w}\| \leqslant \|A\|d|a_n| \leqslant N|a_n|.$$

And so we obtain that $|a_{n+1}/a_n| \leqslant N$, a contradiction. Thus the coordinates of $A^m\mathbf{v}_j$ are contained in $\{a_1, \ldots, a_n\}$ for all $m \geqslant 0$ and $1 \leqslant j \leqslant d$. Thus $\{A^m\mathbf{v}_j \mid m \geqslant 0\}$ is a finite set of vectors. Hence for each j, there exist $a_j < b_j$ such that $A^{a_j}\mathbf{v}_j = A^{b_j}\mathbf{v}_j$. Since A is invertible, we see that $A^{b_j - a_j}\mathbf{v}_j = \mathbf{v}_j$ for $1 \leqslant j \leqslant d$. Let m be the product of $b_j - a_j$ for $1 \leqslant j \leqslant d$. Then $A^m\mathbf{v}_j = \mathbf{v}_j$ for $1 \leqslant j \leqslant d$ and since $\{\mathbf{v}_1, \ldots, \mathbf{v}_d\}$ is a basis for $\mathbb{Q}^d$, we see that A^m is the identity. Hence S has the finite orbit property. □

In Proposition 6, we showed that the finite orbit property is closed under taking unions with finite sets. The following example shows that many closure properties one might hope for do not hold for the finite orbit property.

Example 9. The finite orbit property is not closed under unions, sums, or products.

Let

$$S = \{2^a \mid a \geqslant 1,\ \lfloor \log_2 a \rfloor \text{ is even}\}$$

and let

$$T = \{2^a \mid a \geqslant 1,\ \lfloor \log_2 a \rfloor \text{ is odd}\}$$

for each $n \geqslant 0$, $2^{2^{2n+1}-1} \in S$ and the next smallest integer in S is $2^{2^{2n+2}}$. Since

$$2^{2^{2n+2}}/2^{2^{2n+1}-1} = 2^{2^{2n+1}+1} \to \infty \quad \text{as } n \to \infty,$$

we see that S has the finite orbit property by Proposition 8. Similarly, T, $S \cup \{0\}$, $S \cup \{1\}$ and $T \cup \{0\}$ have the finite orbit property. Observe that $4/(1-4x) = 4 + 16x + 64x^2 + \cdots$ is a rational power series, and so any set containing $\{4, 16, 64, \ldots\}$ cannot have the finite orbit property. Since

$$(S \cup \{0\}) + (T \cup \{0\}) \supseteq S \cup T = \{2, 4, 8, \ldots\} \supseteq \{4, 16, 64, \ldots\},$$

we see that the finite orbit property is neither closed under sum nor union. Consider $S' := (S \cup \{1\}) \cdot (S \cup \{1\})$. We claim that it contains all powers of 4. Certainly if $\lfloor \log_2 2a \rfloor$ is even then 4^a is in S and hence is in S'. If $\lfloor \log_2 2a \rfloor$ is odd then $\lfloor \log_2 a \rfloor$ is even, and so 2^a is in S and so $2^{2a} = 4^a$ is in S'. Thus S' does not have the finite orbit property.

4. Regular sequences

We now show that the connection between the finite orbit property and k-regular sequences.

Theorem 10. *Let S be a set of integers with the finite orbit property and suppose that $\{f(n)\}$ is a k-regular sequence with $f(n) \in S$ for all $n \geqslant 0$. Then $\{f(n)\}$ is k-automatic.*

Proof. Notice that $M(\{f(n)\}; k)$ is a free $\mathbb{Z}$-module of rank d. Let $\{\{h_1(n)\}, \dots, \{h_d(n)\}\}$ be a basis for $V := M(\{f(n)\}; k) \otimes_{\mathbb{Z}} \mathbb{Q}$ with $h_1(n) = f(n)$. Define

$$\mathbf{v}(n) = \begin{bmatrix} h_1(n) \\ \vdots \\ h_d(n) \end{bmatrix}.$$

Then using the k-regular property, we see that there exist $d \times d$ matrices $A_0, \dots, A_{k-1}$ with rational entries such that

$$\mathbf{v}(kn + i) = A_i \mathbf{v}(n). \tag{4.1}$$

Let $\mathcal{X}$ denote the monoid generated by $A_0, \dots, A_{k-1}$. Let

$$T = \big\{\mathbf{v}(n) \mid n \geqslant 0\big\}. \tag{4.2}$$

Observe that

$$T \subseteq S^d$$

and that $\mathrm{Span}_{\mathbb{Q}}\{\mathbf{v} \in T\}$ is $\mathbb{Q}^d$, since otherwise there would exist rational numbers $c_1, \dots, c_d$, not all of which are zero, such that

$$c_1 h_1(n) + \cdots + c_d h_d(n) = 0 \quad \text{for all } n,$$

which contradicts the fact that the sequences $\{h_1(n)\}, \dots, \{h_d(n)\}$ form a basis for V. Since S has the finite orbit property, by Proposition 4 $\mathcal{X}$ is finite. For any a, b with $0 \leqslant b < k^a$, there exists some $X \in \mathcal{X}$ such that the first coordinate of $X\mathbf{v}(n)$ is $h_1(k^a n + b) = f(k^a n + b)$ for all $n \geqslant 0$. Since $\mathcal{X}$ is finite, we see that the set $\{\{f(k^a n + b)\} \mid a \geqslant 0, 0 \leqslant b < k^a\}$ is a finite set of sequences and hence $\{f(n)\}$ is a k-automatic sequence. $\square$

Theorem 11. *Let S be a set of integers. Then the following are equivalent*:

(1) *S has the finite orbit property*;
(2) *any rational power series whose coefficients are eventually in S has the property that its sequence of coefficients is eventually periodic*;
(3) *any rational power series whose coefficients are in S has the property that its sequence of coefficients is eventually periodic*;
(4) *any rational power series whose coefficients are in S has the property that its set of coefficients is finite*;
(5) *any k-regular sequence whose values are eventually in S is necessarily k-automatic*;
(6) *any k-regular sequence whose values are in S is necessarily k-automatic*;
(7) *any k-regular sequence whose values are in S is necessarily bounded.*

Proof. Suppose that (2) is false. Then there is some rational power series whose coefficients are eventually in S whose sequence of coefficients is not eventually periodic. Hence there is a finite set T such that $S \cup T$ does not have the finite orbit property by Proposition 5. Thus S does not have the finite orbit property by Proposition 6. Hence (1) implies (2). Clearly, (2) implies (3) and (3) implies (4). A standard argument shows that (4) implies (3). By Proposition 5, we have that (3) implies (1). Thus we have shown that (1)–(4) are logically equivalent. Next suppose that (5) is false. Then by Theorem 10, there is some finite set T such that $S \cup T$ does not have the finite orbit property. Consequently, S does not have the finite orbit property. It follows that (1) implies (5). Clearly, (5) implies (6), which in turn implies (7). To complete the proof we show that (7) implies (4). Suppose that (4) is false. Let $\sum_{n=0}^{\infty} a_n z^n$ be a rational power series whose coefficients all lie in S and whose set of coefficients is infinite. It is not difficult to show that the sequence $\{f(n)\}$ defined by

$$f(n) = a_m \quad \text{whenever } k^m \leqslant n < k^{m+1}$$

is k-regular. The reason for this is that if $0 \leqslant j < k^i$ and $f(n) = a_m$, then $f(k^i n + j) = a_{m+i}$. The fact that the coefficients of our rational power series satisfy a recurrence then allows us to deduce that $\{f(n)\}$ is k-regular; moreover, this sequence is unbounded. Hence (7) is false if (4) is false. This completes the proof. □

We note that k-regular power series (power series whose sequence of coefficients is k-regular) and rational power series have many properties in common; for example, see Berstel and Reutenauer [3]. Theorem 11 can thus be seen as giving yet another shared characteristic of these two entities. We give, as an application, a corollary which answers question 9 from Section 16.7 of Allouche and Shallit [2].

Corollary 12. *Let $\{f(n)\}$ be an unbounded k-regular sequence. Then $f(n)$ takes on composite values infinitely often.*

Proof. Suppose this is not the case. Let S be the set of primes. Then by assumption $f(n)$ eventually takes values in S and is unbounded. By Theorem 11 this means that S does not have the finite orbit property. But this contradicts Proposition 7. The result follows. □

Acknowledgments

I thank Jean-Paul Allouche and Jeffrey Shallit for many interesting comments. I also thank the referee for many valuable comments and improvements.

References

[1] J.-P. Allouche, J. Shallit, The ring of k-regular sequences, Theoret. Comput. Sci. 98 (1992) 163–197.
[2] J.-P. Allouche, J. Shallit, Automatic Sequences. Theory, Applications, Generalizations, Cambridge University Press, Cambridge, 2003.
[3] J. Berstel, C. Reutenauer, Rational Series and Their Languages, EATCS Monogr. Theoret. Comput. Sci., vol. 12, Springer-Verlag, 1988.
[4] M. Dekking, M. Mendès France, A. van der Poorten, Folds, Math. Intelligencer 4 (3) (1982) 130–138.
[5] M. Dekking, M. Mendès France, A. van der Poorten, Folds. II. Symmetry disturbed, Math. Intelligencer 4 (4) (1982) 173–181.
[6] M. Dekking, M. Mendès France, A. van der Poorten, Folds. III. More morphisms, Math. Intelligencer 4 (4) (1982) 190–195.
[7] G. Hansel, Une démonstration simple du théorème de Skolem–Mahler–Lech, Theoret. Comput. Sci. 43 (1) (1986) 91–98.
[8] C. Lech, A note on recurring series, Ark. Mat. 2 (1953) 417–421.
[9] D. Robinson, A Course in the Theory of Groups, second ed., Grad. Texts in Math., vol. 80, Springer-Verlag, New York, 1996.
[10] M.-P. Schützenberger, On the synchronizing properties of certain prefix codes, Inform. and Control 7 (1964) 23–36.