Invent. math. 168, 175–224 (2007)
DOI: 10.1007/s00222-006-0031-0

Inventiones
mathematicae

A Skolem–Mahler–Lech theorem in positive characteristic and finite automata

Harm Derksen[*]

Department of Mathematics, University of Michigan
(e-mail: hderksen@umich.edu)

Oblatum 6-XII-2006 & 12-XII-2006
Published online: 10 February 2007 – © Springer-Verlag 2007

Abstract. Lech proved in 1953 that the set of zeroes of a linear recurrence sequence in a field of characteristic 0 is the union of a finite set and finitely many infinite arithmetic progressions. This result is known as the Skolem–Mahler–Lech theorem. Lech gave a counterexample to a similar statement in positive characteristic. We will present some more pathological examples. We will state and prove a correct analog of the Skolem–Mahler–Lech theorem in positive characteristic. The zeroes of a recurrence sequence in positive characteristic can be described using finite automata.

Contents

1. Introduction

Suppose that R is a commutative ring (with 1) and M is a (left) R-module. An *infinite M-sequence* is an element in $M^{\mathbb{N}}$, where $\mathbb{N} = \{0, 1, 2, \dots\}$ is the

[*] The author was partially supported by NSF grant, DMS 0349019.

set of nonnegative integers. We say that $a \in M^{\mathbb{N}}$ satisfies an *R-recurrence relation of order d* if there exist $\gamma_0, \gamma_1, \dots, \gamma_{d-1} \in R$ such that

$$a(n+d) = \gamma_{d-1}a(n+d-1) + \gamma_{d-2}a(n+d-2) + \cdots + \gamma_0 a(n) \quad (1)$$

for all $n \in \mathbb{N}$. We will call such a sequence an *R-recurrence sequence*. The smallest nonnegative integer d for which $a \in M^{\mathbb{N}}$ satisfies a recurrence relation of the form (1) is called the *order* of the recurrence sequence a. For a sequence $a \in M^{\mathbb{N}}$ we define its set of zeroes by

$$\mathcal{Z}(a) = \{n \in \mathbb{N} | a(n) = 0\}.$$

An infinite arithmetic progression is a set of the form $m + n\mathbb{N}$ where $m \in \mathbb{N}$ and n a positive integer. The following result is the celebrated Skolem–Mahler–Lech theorem.

Theorem 1.1. *Suppose that K is a field of characteristic* 0 *and $a \in K^{\mathbb{N}}$ is a K-recurrence sequence. Then $\mathcal{Z}(a)$ is the union of a finite set and finitely many infinite arithmetic progressions.*

This theorem was proved by Skolem [28] for $K = \mathbb{Q}$ (the rational numbers), in 1934, by Mahler [16] in 1935 for $K = \overline{\mathbb{Q}}$ (the algebraic numbers) and by Lech for arbitrary fields of characteristic 0 [14,17] in 1953. See also [9, §2.1]. All proofs use an embedding of K into the p-adic completion $\mathbb{Q}_p$ of $\mathbb{Q}$.

It is possible to bound the number of arithmetic progressions, and the size of the finite set in Theorem 1.1 (see [25,27] and [7, Theorem 1.2]). Nevertheless it is still an open problem whether $\mathcal{Z}(a)$ can always be determined for a given K-recurrence sequence $a \in K^{\mathbb{N}}$ where K is a field of characteristic 0. In particular, it is not known if it is decidable whether $\mathcal{Z}(a) = \emptyset$.

The Skolem–Mahler–Lech theorem can be slightly generalized as follows:

Theorem 1.2. *Suppose that R is a commutative $\mathbb{Q}$-algebra, M is a left R-module and $a \in M^{\mathbb{N}}$ is an R-recurrence sequence. Then $\mathcal{Z}(a)$ is the union of a finite set and finitely many infinite arithmetic progressions.*

In this paper we will focus on sequences in fields of positive characteristic. For a prime power q we denote the field with q elements by $\mathbb{F}_q$. We also define $\mathbb{F}_0 = \mathbb{Q}$. Let p be a prime number. It was noted by Lech [14] that the Skolem–Mahler–Lech theorem without any modifications is false in positive characteristic:

Example 1.3. The sequence $a \in \mathbb{F}_p(x)^{\mathbb{N}}$ defined by

$$a(n) = (x+1)^n - x^n - 1$$

is an $\mathbb{F}_p(x)$-recurrence sequence. The sequence satisfies

$$a(n+3) = (2x+2)a(n+2) - (x^2+3x+1)a(n+1) + (x^2+x)a(n)$$

for all $n \in \mathbb{N}$. The zero set

$$\mathcal{Z}(a) = \{p^n | n \in \mathbb{N}\}$$

is clearly not the union of a finite set and a finite number of arithmetic progressions.

Examples such as Example 1.3 do not yet reveal all the pathologies that appear in positive characteristic. The following example is new and stranger.

Example 1.4. Define $a \in \mathbb{F}_p(x, y, z)^{\mathbb{N}}$ by

$$a(n) = (x + y + z)^n - (x + y)^n - (x + z)^n - (y + z)^n + x^n + y^n + z^n.$$

We have (see Proposition 3.2)

$$\mathcal{Z}(a) = \{p^n | n \in \mathbb{N}\} \cup \{p^n + p^m | n, m \in \mathbb{N}\}.$$

In [19], Masser gave similar examples of what he calls "nested Frobenius type solutions" to linear equations over groups in positive characteristic (also called S-unit equations).

In order to describe the zero sets of linear recurrence sequences in positive characteristic, we make the following definition.

Definition 1.5. Let p be a prime number and $q = p^e$ for some positive integer e. Suppose that $d \geq 1$, $c_0, c_1, \ldots, c_d \in \mathbb{Q}$ with $(q - 1)c_i \in \mathbb{Z}$ for all i, $c_0 + c_1 + \cdots + c_d \in \mathbb{Z}$ and $c_i \neq 0$ for $i = 1, 2, \ldots, d$. Then we define

$$\widetilde{S}_q(c_0; c_1, \ldots, c_d) = \left\{c_0 + c_1 q^{k_1} + c_2 q^{k_2} + \cdots + c_d q^{k_d} \middle| k_1, k_2, \ldots, k_d \in \mathbb{N}\right\}$$

and

$$S_q(c_0; c_1, \ldots, c_d) = \widetilde{S}_q(c_0; c_1, \ldots, c_d) \cap \mathbb{N}.$$

The conditions on $c_0, c_1, \ldots, c_d$ imply that

$$\begin{aligned}
&(q - 1)\big(c_0 + c_1 q^{k_1} + c_2 q^{k_2} + \cdots + c_d q^{k_d}\big) \\
&\quad = (q - 1)c_0 + ((q - 1)c_1)q^{k_1} + ((q - 1)c_2)q^{k_2} + \cdots + ((q - 1)c_d)q^{k_d} \\
&\quad \equiv (q - 1)c_0 + (q - 1)c_1 + \cdots + (q - 1)c_d \\
&\quad = (q - 1)(c_0 + c_1 + \cdots + c_d) \equiv 0 \bmod (q - 1).
\end{aligned}$$

It follows that $\widetilde{S}_q(c_0; c_1, \ldots, c_d) \subseteq \mathbb{Z}$. If $c_1, c_2, \ldots, c_d$ are all negative, then $S_q(c_0; c_1, \ldots, c_d)$ is finite.

Definition 1.6. If $c_i > 0$ for some i with $1 \leq i \leq d$, then $S_q(c_0; c_1, \ldots, c_d)$ is called an *elementary p-nested set of order d*. A *p-nested set of order $\leq d$* is a union of a finite set and finitely many elementary p-nested sets of order $\leq d$. A p-nested set of order $\leq d$ is said to have order d if is *not* a p-nested set of order $\leq d - 1$.

We say that two sets S, T are equal *up to a finite set* if the symmetric difference $(S \setminus T) \cup (T \setminus S)$ is finite.

Definition 1.7. We will call a subset of $\mathbb{N}$ *p-normal of order d* if it is, up to a finite set, equal to the union of a p-nested set of order d and finitely many infinite arithmetic progressions.

We are now ready to state the main results of this paper.

Theorem 1.8. *Suppose that K is a field of characteristic $p > 0$. If $a \in K^{\mathbb{N}}$ is a K-recurrence sequence of order d, then $\mathcal{Z}(a)$ is p-normal of order $\leq d - 2$.*

In the proof we will first show that $\mathcal{Z}(a)$ is a p-automatic set (a useful notion from theoretical computer science), using a technique reminiscent of Frobenius splitting. The structure of the automaton that produces $\mathcal{Z}(a)$ turns out to be very special. Using this we will be able to show that $\mathcal{Z}(a)$ is p-normal. Our approach in positive characteristic is entirely different from the techniques in the proof of the Skolem–Mahler–Lech theorem in characteristic 0.

Theorem 1.8 can be generalized to recurrence sequences in modules over commutative $\mathbb{F}_p$-algebras.

Theorem 1.9. *Suppose that p is a prime number, R is a commutative $\mathbb{F}_p$-algebra, M is a left R-module and $a \in M^{\mathbb{N}}$ is an R-recurrence sequence of order d. Then $\mathcal{Z}(a)$ is p-normal of order $\leq d - 2$.*

We will reduce Theorem 1.9 to Theorem 1.8.

An advantage of our proof of Theorem 1.8 is that, unlike in characteristic 0, all the steps in the proof are effective:

Theorem 1.10. *Let p be a prime. Given a field K which is finitely generated over $\mathbb{F}_p$ and a K-recurrence sequence $a \in K^{\mathbb{N}}$, we can effectively determine $\mathcal{Z}(a)$.*

In other words there exists an algorithm which, given K and an explicit recurrence relation for the sequence $a \in K^{\mathbb{N}}$, produces $\mathcal{Z}(a)$ in finite time. The format of the output is an explicit description of $\mathcal{Z}(a)$ in terms of finite sets, arithmetic progressions and elementary p-nested sets as in the definition of a p-normal set (see Definition 1.7).

Some results are known about the density of the zeroes of recurrence sequences in positive characteristic. For a subset $S \subseteq \mathbb{N}$, define

$$\delta_S(n) := \max_{m \in \mathbb{N}} |S \cap \{m, m+1, \ldots, m+n-1\}|.$$

The *upper Banach density* of S is defined by

$$\delta^+(S) = \limsup_{n \to \infty} \frac{\delta(n)}{n}.$$

Suppose that K is a field of characteristic $p > 0$ and $a \in K^{\mathbb{N}}$ is a K-recurrence sequence of order d such that $\mathcal{Z}(a)$ does not contain any infinite arithmetic progressions. It was proved in [3] that $\delta^+(\mathcal{Z}(a)) = 0$. In other words, we have $\delta_{\mathcal{Z}(a)}(n) = o(n)$. (We use here the standard *big O, little o,* Ω, ω notations:

$$\begin{array}{lll} f(n) = O(g(n)) & \text{means} & \limsup_{n\to\infty} |f(n)/g(n)| < \infty, \\ f(n) = o(g(n)) & \text{means} & \lim_{n\to\infty} f(n)/g(n) = 0, \\ f(n) = \Omega(g(n)) & \text{means} & \liminf_{n\to\infty} |f(n)/g(n)| > 0, \\ f(n) = \omega(g(n)) & \text{means} & \lim_{n\to\infty} g(n)/f(n) = 0. \end{array}$$

for any real-valued functions $f, g \in \mathbb{R}^{\mathbb{N}}$.)

Indeed, if $\delta^+(\mathcal{Z}(a)) > 0$, then by Szemerédi's theorem (see [31,8]) $\mathcal{Z}(a)$ contains arithmetic progressions of arbitrary length. But then $\mathcal{Z}(a)$ contains an infinite arithmetic progression (see Corollary 2.2), which contradicts our assumptions. From effective estimates for $\delta_{\mathcal{Z}(a)}(n)$ in [29,30] and [9, Theorem 5.9] it follows that

$$\delta_{\mathcal{Z}(a)}(n) = O(n^{1-\Delta(n)}),$$

where $\Delta(d)$ is defined by $\Delta(2) = 1$ and

$$\Delta(d+1) = \frac{\Delta\left(\lfloor \frac{d}{2} \rfloor + 1\right)}{\lfloor \frac{d}{2} \rfloor + 1}$$

for $d \geq 2$. One can show that $\Delta(d) \geq \exp(-c \log^2(d))$ for some constant c (see [29]). In [9, §2.5] it was suggested that $\delta_{\mathcal{Z}(a)}(n)$ might have a logarithmic upper bound. Although an upper bound $O(\log(n))$ is impossible because of Example 1.4, Theorem 1.8 implies the following result.

Corollary 1.11. *Suppose that K is a field of characteristic $p > 0$ and $a \in K^{\mathbb{N}}$ is an K-recurrence sequence of order d. If $\mathcal{Z}(a)$ does not contain any infinite arithmetic progressions, then*

$$\delta_{\mathcal{Z}(a)}(n) = O(\log(n)^{d-2}).$$

Acknowledgement. I would like to thank Jason Bell for inspiring discussions, Andreas Blass for help on finite automata and regular languages, and Jeff Lagarias, David Masser and the anonymous referee for useful comments.

2. Preliminaries

In this section we give some definitions and elementary facts about linear recurrence sequences. Let R be a ring and M be an R-module. We define the *shift operator* $E : M^{\mathbb{N}} \to M^{\mathbb{N}}$ by

$$(Ea)(n) := a(n+1), \quad n \in \mathbb{N},$$

for all $a \in M^{\mathbb{N}}$. Scalar multiplication makes $M^{\mathbb{N}}$ into a left R-module. Using the shift operator, we may view $M^{\mathbb{N}}$ as a left $R[E]$-module, where $R[E]$ is the polynomial ring over R. Suppose that $a \in M^{\mathbb{N}}$. Then the recurrence relation (1) is equivalent to

$$P(E) \cdot a = 0,$$

where

$$P(E) = E^d - \gamma_{d-1}E^{d-1} - \gamma_{d-2}E^{d-2} - \cdots - \gamma_1 E - \gamma_0.$$

We call $P(E)$ the *companion polynomial* of the recurrence relation (1).

For $j, k \in \mathbb{N}$ we define $L_j^k : \mathbb{N} \to \mathbb{N}$ by

$$L_j^k(n) = kn + j.$$

We define the operator $T_j^k : M^{\mathbb{N}} \to M^{\mathbb{N}}$ by

$$T_j^k a = a \circ L_j^k.$$

So we have

$$\big(T_j^k a\big)(n) = a\big(L_j^k(n)\big) = a(kn + j).$$

Note that $E = T_1^1$. We have the relation

$$ET_j^m = T_j^m E^m. \tag{2}$$

Suppose that R is a commutative ring and $P(T), Q(T) \in R[T]$ are given by

$$P(T) = \alpha_n T^n + \alpha_{n-1}T^{n-1} + \cdots + \alpha_0,$$
$$Q(T) = \beta_m T^m + \beta_{m-1}T^{m-1} + \cdots + \beta_0,$$

where $\alpha_0, \ldots, \alpha_n, \beta_0, \ldots, \beta_m \in R$ and $\alpha_n, \beta_m \neq 0$. We define the *resultant* $\mathrm{Res}_T(P(T), Q(T))$ as the determinant of the matrix

$$\begin{pmatrix}
\alpha_n & \alpha_{n-1} & \cdots & \alpha_0 & & & & \\
 & \alpha_n & \alpha_{n-1} & \cdots & \alpha_0 & & & \\
 & & \ddots & & & & \ddots & \\
 & & & & \alpha_n & \alpha_{n-1} & \cdots & \alpha_0 \\
\beta_m & \beta_{m-1} & \cdots & \beta_0 & & & & \\
 & \beta_m & \beta_{m-1} & \cdots & \beta_0 & & & \\
 & & \ddots & & & & \ddots & \\
 & & & & \beta_m & \beta_{m-1} & \cdots & \beta_0
\end{pmatrix}$$

(see for example [13, IV,§8]).

Lemma 2.1. *If $a \in M^{\mathbb{N}}$ is an R-recurrence sequence of order d, then $T_j^k a$ is an R-recurrence sequence of order $\leq d$.*

Proof. See [9, Theorem 1.3] in the special case where R is a field. We introduce a new auxiliary variable F. Suppose that $P(E) \in R[E]$ is a monic polynomial of degree d such that $P(E) \cdot a = 0$. Define $Q(E), U(E) \in R[E]$ by

$$Q(E) = \mathrm{Res}_F(F^k - E, P(F))$$

and

$$U(E) = \mathrm{Res}_F(F^{k-1} + F^{k-2}E + \cdots + E^{k-1}, P(F)).$$

The polynomials $(-1)^{d(k+1)}Q(E)$ and $(-1)^{d(k+1)}U(E)$ are monic and they have degrees d and $d(k-1)$ respectively. Using

$$F^k - E^k = (F - E)(F^{k-1} + F^{k-2}E + \cdots + E^{k-1})$$

and the multiplicative property of the resultant [13, IX,Theorem 3.10], we get

$$\begin{aligned} Q(E^k) &= \mathrm{Res}_F(F^k - E^k, P(F)) \\ &= \mathrm{Res}_F(F - E, P(F))\, \mathrm{Res}_F(F^{k-1} + F^{k-2}E + \cdots + E^{k-1}, P(F)) \\ &= P(E)U(E). \end{aligned}$$

From (2) it follows that

$$Q(E)T_j^k a = T_j^k Q(E^k)a = T_j^k U(E)P(E)a = 0.$$

Therefore, $T_j^k a$ satisfies a recurrence relation of order d with companion polynomial $(-1)^{d(k+1)}Q(E)$. □

Corollary 2.2. *If $a \in M^{\mathbb{N}}$ is an R-recurrence sequence of order d, and*

$$a(k) = a(k+m) = a(k+2m) = \cdots = a(k+(d-1)m) = 0$$

for some $k \in \mathbb{N}$ and some positive integer m, then

$$a(k+im) = 0$$

for all $i \in \mathbb{N}$.

Proof. The sequence $b = T_k^m a$ is an R-recurrence sequence of order $\leq d$ by Lemma 2.1, and

$$b(0) = b(1) = \cdots = b(d-1) = 0.$$

Using induction and the recurrence relation for b we get $a(k+im) = b(i) = 0$ for all i. □

Let us assume that $M = R = K$ is a field and let $a \in K^{\mathbb{N}}$. The set

$$\operatorname{Ann}(a) = \{P(E) \in K[E] | P(E)a = 0\}$$

is a principal ideal in $K[E]$. Therefore, the ideal $\operatorname{Ann}(a)$ is generated by a unique monic polynomial $P_a(E)$. We call $P_a(E)$ the *minimum polynomial* of the recurrence sequence a. The degree of $P_a(E)$ is exactly the order of the recurrence sequence.

Suppose that

$$P_a(E) = \prod_{i=1}^{r} (E - \alpha_i)^{m_i}, \tag{3}$$

where $\alpha_1, \ldots, \alpha_r$ are dist inct roots in the algebraic closure $\overline{K}$ of K, and $m_1, \ldots, m_r$ are positive integers. Then a has order $d = \sum_{i=1}^{r} m_i$. It is well known that a has the form

$$a(n) = \sum_{i=1}^{r} \sum_{j=0}^{m_i - 1} \beta_{i,j} \binom{n}{j} \alpha_i^n, \quad n \in \mathbb{N}, \tag{4}$$

where $\beta_{i,j} \in \overline{K}$ for all i, j (see for example [9, 1.1.6]). Also, any sequence $a \in K^{\mathbb{N}}$ of the form (4) satisfies a recurrence relation of order $d = \sum_{i=1}^{r} m_i$ and the companion polynomial of this recurrence relation is given by (3).

Definition 2.3. The recurrence sequence a is called

- *basic* if 0 is not a root of $P_a(E)$;
- *nondegenerate* if all roots of $P_a(E)$ are nonzero and the quotient of any two distinct roots is not a root of unity;
- *simple* if all roots of $P_a(E)$ are distinct.

If a is basic, then using the recurrence relation (1) backwards one can define $a(n)$ for all $n \in \mathbb{Z}$. In that case (4) would be valid for all $n \in \mathbb{Z}$ if we interpret

$$\binom{n}{j} = \frac{n(n-1)\cdots(n-j+1)}{j!}$$

as a polynomial of degree j that is defined for all integers n.

If a is simple, then (4) takes a simpler form, namely

$$a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^n, \quad n \in \mathbb{N},$$

where $\beta_1, \ldots, \beta_d \in \overline{K}$.

Lemma 2.4. *Suppose that $a \in K^{\mathbb{N}}$ is a K-recurrence sequence where K is a field.*

(a) *There exists an i such that $E^i a$ is basic.*
(b) *If a is basic, then there exists a positive integer k such that $T_j^k a$ is nondegenerate for all j.*
(c) *If a is basic and K has characteristic $p > 0$, then there exists a positive integer k such that $T_j^k a$ is simple and nondegenerate for all j.*

Proof. Let $P_a(E)$ be the minimum polynomial of a.

(a) We can write $P_a(E) = E^i Q(E)$ where $Q(0) \neq 0$. Then $Q(E)(E^i a) = 0$, hence $E^i a$ is basic.

(b) Let $P_a(E)$ as in (3). There exists a k such that for all $i \neq j$ we have that $(\alpha_i/\alpha_j)^k = 1$ if and only if α_i/α_j is a root of unity. Define $Q(E) = \mathrm{Res}_F(E - F^k, P(F))$ as in the proof of Lemma 2.1. We have $Q(E)(T_j^k a) = 0$ for all j. The roots of $Q(E)$ are $\alpha_1^k, \dots, \alpha_r^k$. In particular, the quotient of any two distinct roots of $Q(E)$ is not a root of unity different from 1. This shows that $T_j^k a$ is nondegenerate for all j.

(c) Let $\gamma_1, \dots, \gamma_s$ be distinct such that

$$\{\gamma_1, \dots, \gamma_s\} = \left\{\alpha_1^k, \dots, \alpha_r^k\right\}.$$

Let q be a power of p such that $q \geq d$. Define $U(E) = \prod_{i=1}^r (E - \gamma_i^q)$. Then $Q(E)$ divides

$$U(E^q) = \prod_{i-1}^{r} \left(E^q - \gamma_i^q\right) = \prod_{i=1}^{r} (E - \gamma_i)^q.$$

Because $P_a(E)$ divides $Q(E^k)$, it divides $U(E^{qk})$ as well. Therefore, for all j we have

$$U(E)\left(T_j^{qk} a\right) = T_j^{qk}(U(E^{qk})a) = 0.$$

Note that $U(E)$ has distinct roots, and any quotient of two distinct roots is not a root of unity. It follows that $T_j^{qk} a$ is simple and nondegenerate for all j. □

Definition 2.5. A *d-balanced* subset of $\mathbb{N}$ is a set of the form

$$\{m_0 + k_1 m_1 + \cdots + k_d m_d | k_1, \dots, k_d \in \{0, 1\}\},$$

where $m_0 \in \mathbb{N}$ and $m_1, \dots, m_d$ are positive integers.

If $m_1 = m_2 = \cdots = m_d$, then

$$\begin{aligned}\{m_0 + k_1 m_1 + \cdots + k_d m_d | k_1, \dots, k_d \in \{0, 1\}\}\\ = \{m_0, m_0 + m_1, m_0 + 2m_1, \dots, m_0 + d m_1\},\end{aligned}$$

so an arithmetic progression of length $d + 1$ is d-balanced.

Lemma 2.6. *Suppose that K is a field and $a \in K^{\mathbb{N}}$ is a nonzero K-recurrence sequence of order d.*

(a) *If K has characteristic 0 and $a \in K^{\mathbb{N}}$ is nondegenerate then $\mathcal{Z}(a)$ does not contain a $(d-1)$-balanced subset.*

(b) *If K has positive characteristic and $a \in K^{\mathbb{N}}$ is simple and nondegenerate, then $\mathcal{Z}(a)$ does not contain a $(d-1)$-balanced subset.*

Proof. Suppose that

$$S := \{m_0 + k_1 m_1 + \cdots + k_d m_d | k_1, \ldots, k_d \in \{0, 1\}\} \subseteq \mathcal{Z}(a).$$

Let

$$P_a(E) = \prod_{i=1}^{d} (E - \alpha_i)$$

be the minimum polynomial of a. Define

$$Q(E) = E^{m_0} \prod_{i=1}^{d-1} \left(E^{m_i} - \alpha_i^{m_i}\right). \tag{5}$$

If $i < d$, then $E - \alpha_d$ does not divide

$$\frac{E^{m_i} - \alpha_i^{m_i}}{E - \alpha_i} = E^{m_i - 1} + \alpha_i E^{m_i - 2} + \cdots + \alpha_i^{m_i - 1}.$$

In case (b), $\alpha_d^{m_i} \neq \alpha_i^{m_i}$ since α_i/α_d is not a root of unity for $i = 1, 2, \ldots, d-1$. In case (a), $\alpha_d^{m_i} = \alpha_i^{m_i}$ implies that $\alpha_d = \alpha_i$. Since K has characteristic 0, $E^{m_i} - \alpha_i^{m_i}$ is square-free, and $E - \alpha_i = E - \alpha_d$ does not divide $(E^{m_i} - \alpha_i^{m_i})/(E - \alpha_i)$.

The polynomial $P_a(E)$ divides $Q(E)(E - \alpha_d)$, but not $Q(E)$. From $(E - \alpha_d)Q(E)a = 0$ it follows that

$$(Q(E)a)(n) = \beta \alpha_d^n$$

for some $\beta \in \overline{K}$. If the coefficient of E^i in $Q(E)$ is nonzero, then (5) implies that $i \in S$ and so, by our supposition, $a(i) = 0$. Since $\beta = (Q(E)a)(0)$ is a linear combination of $a(i)$ $(i \in S)$, it follows that $\beta = 0$. But then $Q(E)a = 0$ and $Q(E)$ must be divisible by the minimum polynomial $P_a(E)$. Contradiction. □

Theorem 1.8 can be reduced to the following theorem for simple nondegenerate sequences.

Theorem 2.7. *If K is a field of characteristic $p > 0$ and $a \in K^{\mathbb{N}}$ is a nonzero simple nondegenerate K-recurrence sequence of order d, then $\mathcal{Z}(a)$ is a p-nested set of order $\leq d-2$.*

Proof of Theorem 1.8. Suppose that $a \in K^{\mathbb{N}}$ is an K-recurrence sequence of order $\leq d$. Without loss of generality we may assume that a is basic, because any linear recurrence sequence can be changed into a basic one by changing only finitely many entries in the sequence. There exist a positive integer k such that $T_j^k a$ is simple and nondegenerate of order $\leq d$ for $j = 0, 1, \ldots, k-1$ by Lemma 2.4 and Lemma 2.1. We have

$$\mathcal{Z}(a) = \bigcup_{j=0}^{k-1} L_j^k\bigl(\mathcal{Z}\bigl(T_j^k a\bigr)\bigr). \tag{6}$$

If $T_j^k a = 0$, then $\mathcal{Z}(T_j^k a) = \mathbb{N}$ and $L_j^k(\mathcal{Z}(T_j^k a)) = L_j^k(\mathbb{N}) = j + k\mathbb{N}$ is an infinite arithmetic progression. Otherwise, $\mathcal{Z}(T_j^k a)$ is a p-nested set of order $\leq d-2$ by Theorem 2.7. But then $L_j^k(\mathcal{Z}(T_j^k a))$ is a union of a finite set and finitely many sets of the form

$$L_j^k(S_q(c_0; c_1, \ldots, c_r)) = S_q(j + kc_0; kc_1, \ldots, kc_r).$$

with q a power of p and $r \leq d-2$, hence $L_j^k(\mathcal{Z}(T_j^k a))$ is p-nested of order $\leq d-2$ for all j. From (6) it follows that $\mathcal{Z}(a)$ is p-normal of order $\leq d-2$ as well. □

3. Examples in positive characteristic

In this section we will concentrate on simple nondegenerate K-recurrence sequences in K where K is a field of positive characteristic. The main idea behind the construction of various pathological examples is the following proposition.

Proposition 3.1. *Assume that K is a field of characteristic $p > 0$ and q is a power of p. Suppose that $a \in K^{\mathbb{N}}$ is given by*

$$a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^n, \quad n \in \mathbb{N},$$

where $\alpha_1, \ldots, \alpha_d, \beta_1, \ldots, \beta_d \in \overline{K}$. If for some $c_0, c_1, \ldots, c_r \in \mathbb{Z}$ the sum

$$\sum_{i=1}^{d} (\beta_i \alpha_i^{c_0}) \otimes \alpha_i^{c_1} \otimes \cdots \otimes \alpha_i^{c_r} \in \underbrace{\overline{K} \otimes_{\mathbb{F}_q} \overline{K} \otimes_{\mathbb{F}_q} \otimes \cdots \otimes_{\mathbb{F}_q} \overline{K}}_{r+1},$$

is equal to 0*, then*

$$S_q(c_0; c_1, \ldots, c_r) \subseteq \mathcal{Z}(a).$$

Proof. Let $\phi : \overline{K} \to \overline{K}$ be the Frobenius map defined by $\phi(\alpha) = \alpha^p$. Define an $\mathbb{F}_q$-linear map

$$\psi : \overline{K} \otimes_{\mathbb{F}_q} \overline{K} \otimes_{\mathbb{F}_q} \cdots \otimes_{\mathbb{F}_q} \overline{K} \to \overline{K}$$

by

$$\gamma_0 \otimes \gamma_1 \otimes \cdots \otimes \gamma_r \mapsto \gamma_0 \gamma_1 \cdots \gamma_r.$$

We have

$$\begin{aligned}
a\big(c_0 + c_1 q^{k_1} + \cdots + c_r q^{k_r}\big) &= \sum_{i=1}^{d} \beta_i \alpha_i^{c_0} \alpha_i^{c_1 q^{k_1}} \alpha_i^{c_2 q^{k_2}} \cdots \alpha_i^{c_r q^{k_r}} \\
&= \sum_{i=1}^{r} \psi\big(\big(\beta_i \alpha_i^{c_0}\big) \otimes \alpha_i^{c_1 q^{k_1}} \otimes \alpha_i^{c_2 q^{k_2}} \otimes \cdots \otimes \alpha_i^{c_r q^{k_r}}\big) \\
&= \sum_{i=1}^{r} \psi\big(\big(\beta_i \alpha_i^{c_0}\big) \otimes \phi^{k_1}\big(\alpha_i^{c_1}\big) \otimes \phi^{k_2}\big(\alpha_i^{c_2}\big) \otimes \cdots \otimes \phi^{k_r}\big(\alpha_i^{c_r}\big)\big) \\
&= \psi\left(\mathrm{id} \otimes \phi^{k_1} \otimes \phi^{k_2} \otimes \cdots \otimes \phi^{k_r} \left(\sum_{i=1}^{r} \big(\beta_i \alpha_i^{c_0}\big) \otimes \alpha_i^{c_1} \otimes \cdots \otimes \alpha_i^{c_r} \right)\right) \\
&= \psi(\mathrm{id} \otimes \phi^{k_1} \otimes \phi^{k_2} \otimes \cdots \otimes \phi^{k_r}(0)) = \psi(0) = 0.
\end{aligned}$$

□

Proposition 3.2. *For the sequence $a \in \mathbb{F}_p(x, y, z)$ defined by*

$$a(n) = (x + y + z)^n - (x + y)^n - (x + z)^n - (y + z)^n + x^n + y^n + z^n,$$

we have

$$\mathcal{Z}(a) = \{p^n | n \in \mathbb{N}\} \cup \{p^n + p^m | n, m \in \mathbb{N}\}.$$

Proof. From

$$\begin{aligned}
&1 \otimes (x + y + z) + (-1) \otimes (x + y) + (-1) \otimes (x + z) \\
&\qquad + (-1) \otimes (y + z) + 1 \otimes x + 1 \otimes y + 1 \otimes z = 0
\end{aligned}$$

in $\mathbb{F}_p(x, y, z) \otimes_{\mathbb{F}_p} \mathbb{F}_p(x, y, z)$ and Proposition 3.1 it follows that

$$S_p(0; 1) = \{1, p, p^2, \ldots\} \subseteq \mathcal{Z}(a).$$

One can also check that

$$\begin{aligned}
&1 \otimes (x + y + z) \otimes (x + y + z) + (-1) \otimes (x + y) \otimes (x + y) \\
&\quad + (-1) \otimes (x + z) \otimes (x + z) + (-1) \otimes (y + z) \otimes (y + z) \\
&\quad + 1 \otimes x \otimes x + 1 \otimes y \otimes y + 1 \otimes z \otimes z = 0
\end{aligned} \tag{7}$$

in $\mathbb{F}_p(x, y, z) \otimes_{\mathbb{F}_p} \mathbb{F}_p(x, y, z) \otimes_{\mathbb{F}_p} \mathbb{F}_p(x, y, z)$. Again from Proposition 3.1 follows that

$$S_p(0; 1, 1) = \{p^n + p^m | n, m \in \mathbb{N}\} \subseteq \mathcal{Z}(a).$$

The other inclusion follows from the more general proposition below. □

The previous proposition is the same as the following one in the case $d = 3$.

Proposition 3.3. *Define $a_d \in \mathbb{F}_p(x_1, \ldots, x_d)^{\mathbb{N}}$ by*

$$a_d(n) := \sum_I (-1)^{d+|I|} \Big(\sum_{i \in I} x_i \Big)^n,$$

where I runs over all nonempty subsets of $\{1, 2, \ldots, d\}$ and $|I|$ denotes the cardinality of I. The sequence a_d satisfies a recurrence relation of order $2^d - 1$. The set $\mathcal{Z}(a_d)$ consists of all sums of at most $d - 1$ powers of p (excluding 0).

Proof. Suppose that $e \leq d - 1$ and $e > 0$. First, we claim that

$$\sum_I (-1)^{d+|I|} \Big(\sum_{i \in I} x_i \Big)^{\otimes e} = 0,$$

where I runs over all subsets of $\{1, 2 \ldots, d\}$ and

$$y^{\otimes e} := \underbrace{y \otimes y \otimes \cdots \otimes y}_{e} \in K^{\otimes e} := K \otimes_{\mathbb{F}_p} K \otimes_{\mathbb{F}_p} \cdots \otimes_{\mathbb{F}_p} K$$

for $y \in K := \mathbb{F}_p(x_1, \ldots, x_d)$. Define a polynomial function $F : K \to K^{\otimes e}$ of degree e by $F(y) := y^{\otimes e}$. For $z \in K$, define an operator Δ_z by $\Delta_z(G)(y) = G(y + z) - G(y)$. Since the operators Δ_z decrease the degree by 1, we have

$$\sum_I (-1)^{d+|I|} \Big(\sum_{i \in I} x_i \Big)^{\otimes e} = (\Delta_{x_d} \Delta_{x_{d-1}} \cdots \Delta_{x_1} F)(0) = 0.$$

By Proposition 3.1, $a_d(n) = 0$ if n is the sum of e powers of p.

Conversely, suppose that n is not the sum of $\leq d - 1$ powers of p. Define $l_1, l_2, \ldots, l_{d-1}$ recursively as follows. For every i, l_i is the largest nonnegative integer such that p^{l_i} divides $n - p^{l_1} - \cdots - p^{l_{i-1}}$.

The coefficient of

$$x_1^{p^{l_1}} x_2^{p^{l_2}} \ldots x_{d-1}^{p^{l_{d-1}}} x_d^{n - p^{l_1} - \ldots - p^{l_{d-1}}} \tag{8}$$

in

$$(x_1 + \cdots + x_d)^n \tag{9}$$

is

$$\binom{n}{p^{l_1}}\binom{n-p^{l_1}}{p^{l_2}}\cdots\binom{n-p^{l_1}-\cdots-p^{l_{d-2}}}{p^{l_{d-1}}}.$$

By Lucas' theorem this coefficient is nonzero. Note that every variable appears in (8). So the coefficient of (8) in $a_d(n)$ is nonzero, therefore $a_d(n)\neq 0$. □

The phenomenon of Proposition 3.2 already appears in recurrence sequences of order 4 as the following example shows.

Example 3.4. Consider the sequence $a\in\mathbb{F}_4(x)^{\mathbb{N}}$ defined by

$$a(n)=x^n+(x+1)^n+(x+\alpha)^n+(x+1+\alpha)^n,$$

where $\alpha\in\mathbb{F}_4\setminus\mathbb{F}_2$. We can compute $a(0)=a(1)=a(2)=0$ and $a(3)=1$. This sequence satisfies a recurrence relation of order 4, whose companion polynomial is

$$(E-x)(E-x-1)(E-x-\alpha)(E-x-1-\alpha)=E^4+E+(x^4+x).$$

The recurrence relation for a is

$$a(n+4)=a(n+1)+(x^4+x)a(n).$$

Note that a is actually a sequence in the subfield $\mathbb{F}_2(x)\subseteq\mathbb{F}_4(x)$.

We have

$$\mathcal{Z}(a)=\{4^n+4^m|n,m\in\mathbb{N}\}\cup\{2\cdot(4^n+4^m)|n,m\in\mathbb{N}\}\cup\{0,1\}.$$

The reader may verify that

$$\begin{aligned}x\otimes x+(x+1)\otimes(x+1)+(x+\alpha)\otimes(x+\alpha)\\+(x+\alpha+1)\otimes(x+\alpha+1)=0\end{aligned}$$

and

$$\begin{aligned}x^2\otimes x^2&+(x+1)^2\otimes(x+1)^2+(x+\alpha)^2\otimes(x+\alpha)^2\\&+(x+\alpha+1)^2\otimes(x+\alpha+1)^2\\&=x^2\otimes x^2+(x^2+1)\otimes(x^2+1)+(x^2+\alpha+1)\otimes(x^2+\alpha+1)\\&+(x^2+\alpha)\otimes(x^2+\alpha)=0\end{aligned}$$

in $\mathbb{F}_4(x)\otimes_{\mathbb{F}_4}\mathbb{F}_4(x)$. Proposition 3.1 implies that $a(4^n+4^m)=0$ and $a(2\cdot(4^n+4^m))=0$ for all $n,m\geq 0$. There reader may also check that $a(0)=a(1)=0$.

If n has at least three 1's in its binary expansion, then we can write

$$n=2^{i_1}+2^{i_2}+\cdots+2^{i_r}$$

with $i_1 < i_2 < \cdots < i_r$ and $r \geq 3$. We can choose a subset $\{j_1, \dots, j_s\} \subseteq \{i_1, \dots, i_r\}$ such that

$$m := 2^{j_1} + 2^{j_2} + \cdots + 2^{j_s}$$

is divisible by 3. The coefficient of $x^{n-m}z^m$ in $(x+z)^n$ is $\binom{n}{m}$, which is odd. If we sum $(x+z)^n$ over $z = 0, 1, \alpha, \alpha+1$, then the coefficient of x^{n-m} is

$$\binom{n}{m}(0^m + 1^m + \alpha^m + (1+\alpha)^m) = \binom{n}{m}(0+1+1+1)$$

which is still odd. This shows that $a(n) \neq 0$. If n is of the form $2 \cdot 4^i + 4^j$ one may take $m = n$ and a similar argument shows that $a(n) \neq 0$.

In the remainder of this section we describe a construction of simple nondegenerate recurrence sequences with many zeroes. Suppose that p is a prime and q is a power of p. For $c_0, c_1, \dots, c_r \in \mathbb{Z}$, we will define a nonzero simple nondegenerate sequence $a \in \mathbb{F}_q(x)^{\mathbb{N}}$ such that

$$S_q(c_0; c_1, \dots, c_r) \subseteq \mathcal{Z}(a)$$

Let $\gamma_1(x), \gamma_2(x), \dots, \gamma_{s(d)}(x)$ be all the irreducible polynomials in $\mathbb{F}_q[x]$ of degree $\leq d$. Define

$$\mathcal{C}_d := \left\{ \prod_{i=1}^{s(d)} \gamma_i(x)^{e_i} \middle| e_i \in \{0,1\} \text{ for all } i \right\}.$$

The set $\mathcal{C}_d$ has $2^{s(d)}$ elements. Let $\mathbb{F}_q[x]_{\leq e}$ be the space of polynomials of degree $\leq e$. Define $\mathcal{M}_{d,c}$ as the $\mathbb{F}_q$-vector space spanned by all $\gamma(x)^c$ with $\gamma(x) \in \mathcal{C}_d$. If c is a nonnegative integer, then $\mathcal{M}_{d,c}$ is contained in $\mathbb{F}_q[x]_{\leq cds(d)}$ and therefore

$$\dim \mathcal{M}_{d,c} \leq \dim \mathbb{F}_q[x]_{\leq cds(d)} = cds(d) + 1.$$

If $c < 0$ then $\mathcal{M}_{d,c}$ is contained in $\mathcal{M}_{d,-c}(\prod_{i=1}^{s(d)} \gamma_i(x)^c)$. So we have

$$\dim \mathcal{M}_{d,c} \leq |c|ds(d) + 1$$

for all integers c. For all $c \in \mathbb{Z}$, the inequality

$$\dim \mathbb{F}_q[x]_{\leq e}\mathcal{M}_{d,c} \leq |c|ds(d) + e + 1$$

holds. Consider the vector space

$$V_{d,e} = \mathbb{F}_q[x]_{\leq e}\mathcal{M}_{d,c_0} \otimes_{\mathbb{F}_q} \mathcal{M}_{d,c_1} \otimes_{\mathbb{F}_q} \mathcal{M}_{d,c_2} \otimes_{\mathbb{F}_q} \cdots \otimes_{\mathbb{F}_q} \mathcal{M}_{d,c_r}.$$

We have

$$\dim V_{d,e} \leq (|c_0|ds(d) + e + 1) \prod_{i=1}^{r} (|c_i|ds(d) + 1).$$

Let $\mathcal{B}_{d,e} \subseteq V_{d,e}$ be the subset of all

$$(x^i \gamma(x)^{c_0}) \otimes \gamma(x)^{c_1} \otimes \cdots \otimes \gamma(x)^{c_r}$$

with $0 \leq i \leq e$ and $\gamma(x) \in \mathcal{C}_d$. The set $\mathcal{B}_{d,e}$ has cardinality $|\mathcal{B}_{d,e}| = (e+1)2^{s(d)}$.

Note that $\lim_{d \to \infty} s(d) = \infty$. We have

$$|\mathcal{B}_{d,e}| > \dim V_{d,e}$$

for $d \gg 0$ because $|\mathcal{B}_{d,e}|$ depends at least exponentially on $s(d)$ and $\dim V_{d,e}$ depends at most polynomially on $s(d)$. For d large enough, $\mathcal{B}_{d,e}$ will be dependent. This means that there exist polynomials $v_\gamma(x) \in \mathbb{F}_q[x]$, of degree $\leq e$, not all 0, such that

$$\sum_{\gamma(x) \in \mathcal{C}_d} \left(v_\gamma(x)\gamma(x)^{c_0}\right) \otimes \gamma(x)^{c_1} \otimes \cdots \otimes \gamma(x)^{c_r} = 0.$$

From Proposition 3.1 it follows that

$$S_q(c_0; c_1, \ldots, c_r) \subseteq \mathcal{Z}(a),$$

where $a \in \mathbb{F}_q[x]^{\mathbb{N}}$ is defined by

$$a(n) = \sum_{\gamma(x) \in \mathcal{C}_d} v_{\gamma(x)}\gamma(x)^n.$$

Conjecture 3.5. If we choose e and d large enough, then there exists a choice for the $\{v_{\gamma(x)}\}$ such that

$$S_q(c_0; c_1, \ldots, c_r) = \mathcal{Z}(a).$$

Perhaps instead of choosing the $v_{\gamma(x)} \in \mathbb{F}_q[x]_{\leq e}$ one should choose them in $K[x]_{\leq e}$ where K is a field extension of $\mathbb{F}_q$ containing many transcendental elements.

The converse of Theorem 1.8 is not true. For example, consider the 2-normal set

$$S = \{2^n | n \in \mathbb{N}\} \cup \{2^n + 2^m | n, m \in \mathbb{N}\} = \{1\} \cup \{2^n + 2^m | n, m \in \mathbb{N}\}.$$

The set S is 2-normal of order 2. However, there does not exist a recurrence sequence $a \in K^{\mathbb{N}}$ with $\mathcal{Z}(a) = S$ of order ≤ 4. Note that S contains $\{1, 2, 3, 4, 5, 6\}$ which is an arithmetic progression of length 6. Suppose that $a \in K^{\mathbb{N}}$ is a K-recurrence sequence where K is a field of characteristic 2. If $\mathcal{Z}(a) = S$, then $\mathcal{Z}(a)$ does not contain an infinite arithmetic progression and a has order ≥ 7 by Corollary 2.2. However, we do conjecture the following weaker converse.

Conjecture 3.6. If S is a p-normal set, then there exists a field K of characteristic p and a K-recurrence sequence $a \in K^{\mathbb{N}}$ such that $\mathcal{Z}(a) = S$.

Lemma 3.7. *Conjecture 3.5 implies Conjecture 3.6.*

Proof. Suppose Conjecture 3.5 is true. We will prove Conjecture 3.6. If we change finitely many entries in a recurrence sequence then the sequence remains a recurrence sequence. It follows that if S, T are equal up to a finite set and T is the zero set of a recurrence sequence in $K^{\mathbb{N}}$, then so is S. Without loss of generality we may assume that S is a union of finitely many infinite arithmetic progressions and a p-nested set.

Note that if $a, b \in K^{\mathbb{N}}$ are K-recurrence sequences, then so is the product ab defined by $ab(n) = a(n)b(n)$. In particular

$$\mathcal{Z}(ab) = \mathcal{Z}(a) \cup \mathcal{Z}(b).$$

So we easily reduce to the case where S is either an arithmetic progression, or an elementary p-nested set.

For any arithmetic progression it is easy to find a recurrence sequence with that particular zero set. Suppose that $S = S_q(c_0; c_1, \dots, c_r)$. If $c_0, \dots, c_r$ are all integers then Conjecture 3.5 implies Conjecture 3.6. Otherwise, we still have that $(q-1)c_i \in \mathbb{Z}$ for all i. There exists a K-recurrence sequence $a \in K^{\mathbb{N}}$ such that

$$\mathcal{Z}(a) = S_q((q-1)c_0; (q-1)c_1, \dots, (q-1)c_r)$$

by Conjecture 3.5. Define $b \in K^{\mathbb{N}}$ by $b(n) = a((q-1)n)$ for all $n \in \mathbb{N}$, i.e., $b = T_0^{q-1}a$. It follows that

$$\begin{aligned}\mathcal{Z}(b) &= \left(L_0^{q-1}\right)^{-1}(\mathcal{Z}(a))\\ &= \left(L_0^{q-1}\right)^{-1}(S_q((q-1)c_0; (q-1)c_1, \dots, (q-1)c_r))\\ &= S_q(c_0; c_1, \dots, c_r).\end{aligned}$$

□

4. p-automatic sequences

We first give the necessary definitions for finite automata. Let p be a positive integer and define the *alphabet* $\mathcal{A} = \{0, 1, 2, \dots, p-1\}$. Let $\mathcal{A}^\star$ be the set of all finite words in the alphabet $\mathcal{A}$ (including the empty word). A subset $\mathcal{L} \subseteq \mathcal{A}^\star$ is called a *language*.

Definition 4.1 (See [15, §1.9]). The collection of *regular* languages $\mathcal{R}$ is the smallest subcollection of the collection of all languages such that

(1) $\emptyset \in \mathcal{R}$, and $\{v\} \in \mathcal{R}$ for all $v \in \mathcal{A}$;
(2) If $L, M \in \mathcal{R}$, then $L \cup M \in \mathcal{R}$, $L \circ M \in \mathcal{R}$ (the set of all concatenations of a word in L and a word in M).
(3) If $L \in \mathcal{R}$, then $L^\star \in \mathcal{R}$ where $L^\star$ is the Kleene closure, i.e., the set of all words obtained by concatenating a finite number of words from L.

For a word w and a positive integer k we denote the concatenation

$$\underbrace{ww\cdots w}_{k}$$

of k copies of w by w^k. We also define w^0 as the empty word.

Definition 4.2. A *finite automaton* with alphabet $\mathcal{A}$ is a finite set $\mathcal{V}$ called the *set of states*, an initial state $I \in \mathcal{V}$, a set of final states $\mathcal{F} \subseteq \mathcal{V}$ together with a map

$$\tau : \mathcal{V} \times \mathcal{A} \to \mathcal{V}.$$

We will write $S \cdot t$ instead of $\tau(S, t)$ for $t \in \mathcal{A}$ and $S \in \mathcal{V}$. For a word $w = t_r t_{r-1} \cdots t_0$ we inductively define

$$S \cdot w = S \cdot t_r t_{r-1} \cdots t_0 := (S \cdot t_r) \cdot (t_{r-1} t_{r-2} \cdots t_0).$$

This way, we may view τ as a right action of the monoid $\mathcal{A}^\star$ on $\mathcal{V}$. We say that the automaton *accepts* the word w if $I \cdot w \in \mathcal{F}$.

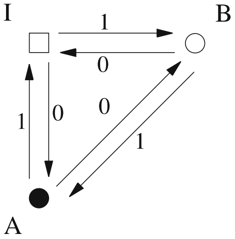
Theorem 4.3 (See [15, Theorem 2.5.1]). *A language $\mathcal{L}$ is regular if and only if it is the set of accepted words for some automaton.*

An automaton can be represented by a graph. The set of vertices are labeled by $\mathcal{V}$. For each state $S \in \mathcal{V}$ and each $i \in \mathcal{A}$ we draw an arrow from S to $S \cdot i$ with label i. The initial state vertex we will draw as a square and the other state vertices as circles. Final states will be indicated by solid circles or a solid square (if a final state coincides with the initial state) while non-final states are open circles or an open square (if the initial state is not a final state).

Example 4.4. Consider an automaton for $p = 2$ with $\mathcal{V} = \{I, A, B\}$ where I is an initial state and A and B are two other states. The set of final states is $\mathcal{F} = \{A\}$. We define $\tau : \mathcal{V} \times \{0, 1\} \to \mathcal{V}$ by $I \cdot 0 = A$, $I \cdot 1 = B$, $A \cdot 0 = B$, $A \cdot 1 = I$, $B \cdot 0 = I$ and $B \cdot 1 = A$. The set of accepted words is

$$\mathcal{L} = \{0, 11, 001, 010, 100, 0000, 0111, 1011, 1101, 1110, \dots\}.$$

In fact, $\mathcal{L}$ is the set of all words for which the number of 0's minus the number of 1's is congruent 1 modulo 3. The graph of the automaton is as follows:



Words in the alphabet $\mathcal{A}$ can be viewed as nonnegative integers written in base p. For a word $w = t_r t_{r-1} \cdots t_0$ we define

$$[w]_p = t_r p^r + t_{r-1} p^{r-1} + \cdots + t_0.$$

For a nonnegative integer $n \in \mathbb{N}$ there exists a unique word $w = t_r t_{r-1} \cdots t_0 \in \mathcal{A}^\star$ with $t_r \neq 0$ and $n = [w]_p$.

Definition 4.5. A subset of $S \subseteq \mathbb{N}$ is called *p-automatic* if there exists an automaton such that a word $w \in \mathcal{A}^\star$ is accepted if and only if $[w]_p \in S$. We call such an automaton an *automaton that produces* S.

In other words, $S \subseteq \mathbb{N}$ is p-automatic if and only if the language $\{w | [w]_p \in S\}$ is regular by Theorem 4.3. Note that such an automaton accepts a word w if and only if it accepts the word $0w$. Without loss of generality one may assume that $I \cdot 0 = I$.

If $w = t_r t_{r-1} \cdots t_0$ is a word, then the reverse word w^{rev} is defined by

$$w^{\text{rev}} := t_0 t_1 \cdots t_r.$$

We also define

$$w \cdot S = S \cdot w^{\text{rev}} \tag{10}$$

for any word $w \in \mathcal{A}^\star$ and any state $S \in \mathcal{V}$. This way, we can view $\mathcal{A}^\star$ as a monoid acting on the *left* on $\mathcal{V}$.

Definition 4.6. A subset of $S \subseteq \mathbb{N}$ is called *reversely p-automatic* if there exists an automaton such that a word $w \in \mathcal{A}^\star$ is accepted if and only if $[w^{\text{rev}}]_p \in S$. We call such an automaton an *automaton that produces S reversely.*

Lemma 4.7. *A subset of $S \subseteq \mathbb{N}$ is p-automatic if and only if it is reversely p-automatic.*

Proof. Let $\mathcal{L} = \{w \in \mathcal{A}^\star | [w]_p \in S\}$. Now S is p-automatic if and only if $\mathcal{L}$ is regular, and S is reversely p-automatic if and only if

$$\mathcal{L}^{\text{rev}} := \{w^{\text{rev}} | w \in \mathcal{L}\}$$

is regular. It is clear from the symmetry in Definition 4.1 that $\mathcal{L}$ is regular if and only if $\mathcal{L}^{\text{rev}}$ is regular. (I thank Andreas Blass for pointing this out to me.) □

Suppose that a p-automaton produces $S \subseteq \mathbb{N}$ reversely. Then the set $(L_t^p)^{-1}(S)$ is also p-automatic. Indeed, if instead of I, we take $I \cdot t$ as initial state, then the automaton will reversely produce $(L_t^p)^{-1}(S)$ instead of S. If $w = t_r t_{r-1} \cdots t_0$ is a word, then

$$\begin{aligned}\left(L_{t_r}^p\right)^{-1}\left(L_{t_{r-1}}^p\right)^{-1} \cdots \left(L_{t_0}^p\right)^{-1}(S) &= \left(L_{t_0}^p L_{t_1}^p \cdots L_{t_r}^p\right)^{-1}(S) \\ &= \left(L_{[t_r t_{r-1} \cdots t_0]_p}^{p^{r+1}}\right)^{-1}(S)\end{aligned}$$

is p-automatic as well. It is reversely produced by the same automaton that produces S except that we change the initial state to $I \cdot t_0 t_1 \cdots t_r$. Since there are only finitely many states, we get the following corollary.

Corollary 4.8. *If $S \subseteq \mathbb{N}$ is p-automatic then the set*

$$\mathcal{V}_S := \left\{ \left(L_i^{p^r}\right)^{-1}(S) \middle| r \in \mathbb{N}, 0 \leq i < p^r \right\}$$

is finite.

We will also prove the converse. Suppose that $\mathcal{V}_S$ is finite for some $S \subseteq \mathbb{N}$. Rather than constructing an automaton that produces S, we will construct an automaton that produces S reversely. In fact, we can do this in a canonical way. For the set of states we take $\mathcal{V}_S$. For the initial state we take $I := S$. For $t \in \mathcal{A}$ and $U \in \mathcal{V}_S$ we define $U \cdot t := (L_t^p)^{-1}(U)$. The set of final states is

$$\mathcal{F}_S := \{U \in \mathcal{V}_S | 0 \in U\}.$$

A word $w = t_0 t_1 \ldots t_r \in \mathcal{A}^\star$ is accepted by this automaton if and only if

$$\begin{aligned} S \cdot t_0 t_1 \cdots t_r &= \left(L_{t_r}^p\right)^{-1} \left(L_{t_{r-1}}^p\right)^{-1} \cdots \left(L_{t_0}^p\right)^{-1}(S) \\ &= \left(L_{[t_r t_{r-1} \cdots t_0]_p}^{p^{r+1}}\right)^{-1}(S) = \left(L_{[w^{\text{rev}}]_p}^{p^{r+1}}\right)^{-1}(S) \end{aligned}$$

contains 0. Therefore w is accepted if and only if $[w^{\text{rev}}]_p \in S$.

Proposition 4.9. *The converse of Corollary 4.8 is true: if $\mathcal{V}_S$ is finite, then S is p-automatic. The automaton constructed above has the smallest number of states (namely $|\mathcal{V}_S|$) among all automata that produce S reversely.*

Proof. Suppose that $\mathcal{V}_S$ is finite. We already constructed an automaton that produces S reversely whose set of states is $\mathcal{V}_S$. Assume that we have another automaton that produces S reversely. Suppose that this automaton is given by the set of states $\mathcal{V}$, the initial state $I \in \mathcal{V}$, a set of final states $\mathcal{F} \subseteq \mathcal{V}$ and

$$\tau : \mathcal{V} \times \mathcal{A} \to \mathcal{V}.$$

By definition $w \cdot I \in \mathcal{F}$ if and only if $[w]_p \in S$. Without loss of generality we may assume that each state in $\mathcal{V}$ can be reached by a path from I. We define a map $\psi : \mathcal{V} \to \mathcal{V}_S$ as follows. For any state $R \in \mathcal{V}$ we define

$$\psi(R) = \{[w]_p | w \cdot R \in \mathcal{F}\}.$$

If $R = u \cdot I$ and u has length r then

$$[wu]_p \in S \Leftrightarrow wu \cdot I \in \mathcal{F} \Leftrightarrow w \cdot R \in \mathcal{F} \Leftrightarrow [w]_p \in \psi(R).$$

It follows that

$$\psi(R) = \left(L_{[u]_p}^{p^r}\right)^{-1}(S) \in \mathcal{V}_S.$$

From this it is easy to see that ψ is well-defined and surjective. □

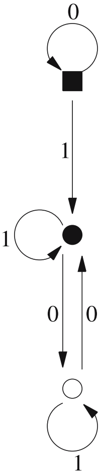
Example 4.10. Suppose that

$$S = \{0, 1, 3, 4, 7, 9, 10, 12, 16, \dots\} \subseteq \mathbb{N}$$

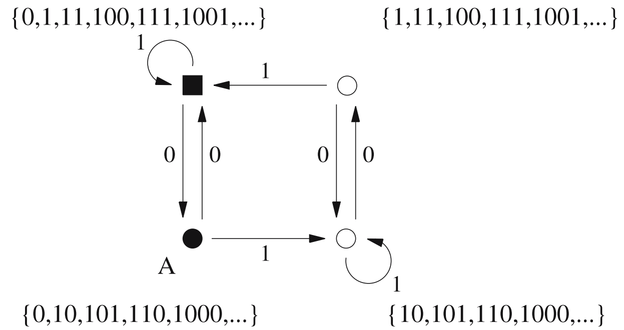
is the subset of all nonnegative integers which have an even number of 0's in their binary expansion, together with 0. If we write integers in base 2 we have

$$S = \{0, 1, 11, 100, 111, 1001, 1010, 1100, \dots\}.$$

The set S is 2-automatic. An automaton that produces S is for example:



The set $\mathcal{V}_S$ contains 4 elements. The first element is S itself. The set $(L_0^2)^{-1}(S)$ consists of all positive integers with an odd number of zeroes in their binary expansion together with 0. The set $(L_2^4)^{-1}(S)$ is the set of all *positive* integers with an odd numbers of zeroes in their binary expansion. Finally, the set $(L_2^8)^{-1}(S)$ consists of all positive integers with an even number of zeroes in their binary expansion. Using the set $\mathcal{V}_S$ we construct an automaton that produces S reversely. The graph of the automaton is as follows:



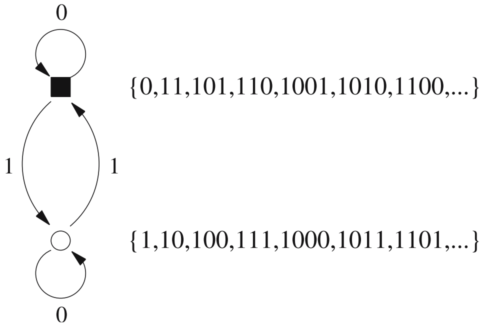
Example 4.11. Let $p = 2$ and let

$$S = \{0, 3, 5, 6, 9, 10, 12, 15, 31, \dots\}$$

be the set of all nonnegative integers which have an even number of 1's in their base 2 expansion. In base 2 we get

$$S = \{0, 11, 101, 110, 1001, 1010, 1100, 1111, 10001, \dots\}.$$

The automaton producing S reversely is as follows:



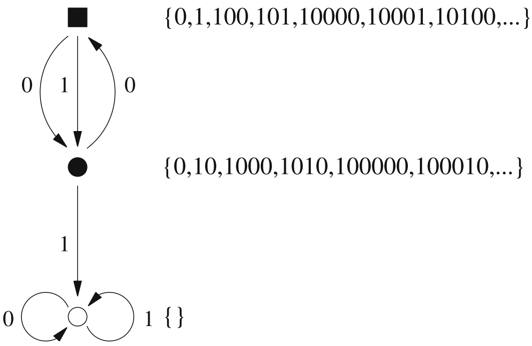
Example 4.12. Let $p = 2$ and let S be the set of all nonnegative integers which have only 0's and 1's in their base 4 extension. We have

$$S = \{0, 1, 4, 5, 16, 17, 20, 21, \dots\}$$

and

$$S = \{0, 1, 100, 101, 10000, 10001, 10100, 10101, \dots\}$$

in base 2. The automaton producing S reversely is as follows:



Lemma 4.13. *Suppose that $S \subseteq \mathbb{N}$ is a subset and N is a positive integer. Then S is p-automatic if and only if $(L_j^N)^{-1}(S)$ is p-automatic for $j = 0, 1, 2, \dots, N-1$.*

Proof. The set S is p-automatic if and only if

$$\left\{\left(L_j^N\right)^{-1}\left(L_i^{p^e}\right)^{-1}(S)\middle| e \in \mathbb{N}, 0 \leq i < p^e, 0 \leq j < N\right\} \tag{11}$$

is finite. On the other hand $(L_k^N)^{-1}(S)$ is p-automatic for $k = 0, 1, \ldots, N-1$ if and only if

$$\left\{\left(L_l^{p^e}\right)^{-1}\left(L_k^N\right)^{-1}(S)| e \in \mathbb{N}, 0 \leq l < p^e, 0 \leq k < N\right\} \tag{12}$$

is finite. If $p^e j + i = Nl + k$ with $0 \leq i, l < p^e$ and $0 \leq j, k < N$ then we have

$$L_i^{p^e} L_j^N = L_{p^e j+i}^{Np^e} = L_{Nl+k}^{Np^e} = L_k^N L_l^{p^e}.$$

It follows that (11) and (12) are the same. □

The previous lemma shows that any arithmetic progression is p-automatic. A major step toward the proof of Theorem 1.8 is the following result.

Theorem 4.14. *If K is a field of characteristic $p > 0$ and $a \in K^{\mathbb{N}}$ is a recurrence sequence, then the set $\mathcal{Z}(a)$ is p-automatic.*

The next section is dedicated to the proof of Theorem 4.14.

5. Free Frobenius splitting

Suppose that K is a finitely generated field over $\mathbb{F}_p$. For any subset V of K we define

$$V^{\langle p\rangle} = \{f^p | f \in V\}.$$

If V is an $\mathbb{F}_p$-subspace of K, then so is $V^{\langle p\rangle}$. For $\mathbb{F}_p$ subspaces V and W of K, the $\mathbb{F}_p$-vector space spanned by all products vw with $v \in V$ and $w \in W$ will be denoted by VW. For $\alpha \in \mathbb{R}$ we denote the largest integer $\leq \alpha$ by $\lfloor\alpha\rfloor$.

Lemma 5.1. *Suppose that V is an n-dimensional $\mathbb{F}_p$-subspace of K containing* 1. *Then we have*

$$V^l \subseteq (V^{\lfloor l/p\rfloor})^{\langle p\rangle} V^{n(p-1)}.$$

Proof. Let $e_1, \ldots, e_n$ be a basis of V. Then V^l is spanned by monomials in $e_1, \ldots, e_n$ of degree l. Let

$$f = e_1^{a_1} e_2^{a_2} \cdots e_n^{a_n}$$

be such a monomial. We can write $a_i = pb_i + c_i$ with $0 \leq c_i \leq (p-1)$. Then we have

$$f = u^p v,$$

where $u = \prod_i e_i^{b_i} \in V^{\lfloor l/p\rfloor}$ and $v = \prod_i e_i^{c_i} \in V^{n(p-1)}$. □

Let $K^{\langle p\rangle} = \{f^p | f \in K\}$ be the subfield of K of all p-th powers. The field extension $K \supset K^{\langle p\rangle}$ has finite degree, say m, and we can write

$$K = K^{\langle p\rangle}h_1 \oplus K^{\langle p\rangle}h_2 \oplus \cdots \oplus K^{\langle p\rangle}h_m$$

for certain $h_1, h_2, \ldots, h_m \in K$. Define $\pi_1, \pi_2, \ldots, \pi_m : K \to K$ by

$$f = \sum_{i=1}^{m} \pi_i(f)^p h_i$$

for all $f \in K$. Note that $\pi_i(g^p f) = g\pi_i(f)$ for all $h, f \in K$.

Proposition 5.2. *Suppose that $V \subseteq K$ is a finite dimensional $\mathbb{F}_p$-subspace. Then there exists a finite dimensional $\mathbb{F}_p$-subspace W of K containing V such that*

$$\pi_i(VW) \subseteq W$$

for all i.

Proof. Without loss of generality we may assume that V contains $1, h_1, \ldots, h_m$ and generators of the field K over $\mathbb{F}_p$. Let R be the ring generated by V. We have

$$R \supseteq R^{\langle p\rangle}h_1 \oplus R^{\langle p\rangle}h_2 \oplus \cdots \oplus R^{\langle p\rangle}h_m.$$

The module $M = R/(R^{\langle p\rangle}h_1 \oplus R^{\langle p\rangle}h_2 \oplus \cdots \oplus R^{\langle p\rangle}h_m)$ is a finitely generated torsion $R^{\langle p\rangle}$-module. There exists a nonzero $g \in R$, such that $g^p M = 0$. If we localize with respect to g we get

$$R_g = R_{g^p} = (R_g)^{\langle p\rangle}h_1 \oplus \cdots \oplus (R_g)^{\langle p\rangle}h_m.$$

Without loss of generality we may assume that V contains g^{-1}.

The above discussion shows that we only have to prove the proposition in the case where the ring R generated by V satisfies

$$R = R^{\langle p\rangle}h_1 \oplus \cdots \oplus R^{\langle p\rangle}h_m. \tag{13}$$

Let $n := \dim_{\mathbb{F}_p} V$. By Lemma 5.1 we have

$$V^l \subseteq (V^{\lfloor l/p\rfloor})^{\langle p\rangle} V^{n(p-1)}. \tag{14}$$

From (13) it follows that there exists a constant C such that

$$V^{n(p-1)} \subseteq (V^C)^{\langle p\rangle}h_1 \oplus \cdots \oplus (V^C)^{\langle p\rangle}h_m. \tag{15}$$

Combining (14) and (15) gives

$$V^l \subseteq (V^{C+\lfloor l/p\rfloor})^{\langle p\rangle} h_1 \oplus \cdots \oplus (V^{C+\lfloor l/p\rfloor})^{\langle p\rangle} h_m.$$

If $l > Cp/(p-1)$ then

$$C + \left\lfloor \tfrac{l}{p} \right\rfloor \leq C + \tfrac{l}{p} < \tfrac{l(p-1)}{p} + \tfrac{l}{p} = l$$

which implies that

$$V^l \subseteq (V^{l-1})^{\langle p\rangle} h_1 \oplus \cdots \oplus (V^{l-1})^{\langle p\rangle} h_m.$$

So we may take $W = V^{l-1}$. □

Proof of Theorem 4.14. If we change finitely many entries in the sequence a then $\mathcal{Z}(a)$ remains unchanged up to a finite set. Without loss of generality we may assume that a is basic by changing finitely many entries in a. In regard of Lemma 4.13 and Lemma 2.4 we may also assume that a is simple and nondegenerate. This means that we can write (after enlarging K)

$$a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^n$$

with $\alpha_1, \ldots, \alpha_d, \beta_1, \ldots, \beta_d \in K \setminus \{0\}$. We may assume without loss of generality that $\alpha_1, \ldots, \alpha_d$ are distinct. Let $V \subseteq K$ be the $\mathbb{F}_p$-space spanned by all α_i^j with $0 \leq j < p$ and all β_i. Let W be as in the Proposition 5.2. Define $a_i = (\alpha_i^0, \alpha_i^1, \ldots)$. Then we can write

$$a = \beta_1 a_1 + \beta_2 a_2 + \cdots + \beta_r a_d.$$

Consider the $\mathbb{F}_q$-vector space

$$U = Wa_1 + Wa_2 + \cdots + Wa_d \subseteq W^{\mathbb{N}}$$

(this is in fact a direct sum). We claim that

$$\pi_i\big(T_j^p U\big) \subseteq U$$

for all $i \in \{1, 2, \ldots, m\}$ and all $j \in \{0, 1, \ldots, p-1\}$. We have

$$\begin{aligned}\pi_i T_j^p(Wa_k) &= \pi_i T_j^p\big(W\big(\alpha_k^0, \alpha_k^1, \ldots\big)\big) = \pi_i\big(W\big(\alpha_k^j, \alpha_k^{j+p}, \alpha_k^{j+2p}, \ldots\big)\big)\\ &= \pi_i\big((W\alpha^j)\big(\alpha_k^0, \alpha_k^p, \ldots\big)\big) \subseteq \pi_i(WV)\big(\alpha_k^0, \alpha_k^1, \alpha_k^2, \ldots\big) \subseteq Wa_k.\end{aligned}$$

This proves that $\pi_i(T_j^p U) \subseteq U$.

Let $\mathcal{W}$ be the set of all

$$\mathcal{Z}(b_1) \cap \cdots \cap \mathcal{Z}(b_r)$$

with $r \in \mathbb{N}$ and $b_1, \ldots, b_r \in U$. If $S \in \mathcal{W}$, then

$$S = \mathcal{Z}(c_1) \cap \cdots \cap \mathcal{Z}(c_t)$$

for some $c_1, \ldots, c_t \in U$. Now we get

$$\left(L_i^p\right)^{-1}(S) = \bigcap_{j=1}^{t} \left(L_i^p\right)^{-1}(\mathcal{Z}(c_j))$$

and

$$\left(L_i^p\right)^{-1}(\mathcal{Z}(c_j)) = \mathcal{Z}\left(T_i^p c_j\right) = \mathcal{Z}\left(\pi_1\left(T_i^p c_j\right)\right) \cap \cdots \cap \mathcal{Z}\left(\pi_m\left(T_i^p c_j\right)\right) \in \mathcal{W}$$

for all j because $\pi_l(T_i^p c_j) \in U$ for all l and j. We obtain $(L_i^p)^{-1}(S) \in \mathcal{W}$ because $\mathcal{W}$ is closed under intersections. This shows that $\mathcal{W}$ is closed under the operations $S \mapsto (L_i^p)^{-1}(S)$ for $i = 0, 1, \ldots, p-1$. Because $\mathcal{Z}(a) \in \mathcal{W}$ we get

$$\mathcal{V}_{\mathcal{Z}(a)} \subseteq \mathcal{W}.$$

Since $\mathcal{W}$ is finite, so is $\mathcal{V}_{\mathcal{Z}(a)}$. We conclude that $\mathcal{Z}(a)$ is p-automatic. □

6. Bounds for zero sets

In this section we find explicit bounds for the zero set of recurrence sequences in positive characteristic. The following sections do not depend on this section, so the reader may skip this section.

Definition 6.1. Suppose that $S \subseteq \mathbb{N}$ is a p-automatic set. We define the *p-complexity of S* by

$$\mathrm{comp}_p(S) := |\mathcal{V}_S|,$$

where $\mathcal{V}_S$ is as in Corollary 4.8.

The p-complexity is a useful measure for complexity of a p-automatic set as the following lemmas show.

Lemma 6.2. *If $m \in S$ and S is finite, then $m < p^{\mathrm{comp}_p(S)-2}$.*

Proof. Without loss of generality we may assume that m is the largest element of S. If $m = 0$ then $S = \{0\}$ and $\mathcal{V}_S = \{\{0\}, \emptyset\}$. In this case $\mathrm{comp}_p(S) = 2$ and

$$m = 0 < 1 = p^0 = p^{\mathrm{comp}_p(S)-2}.$$

Suppose that $m = [w_r \cdots w_0]_p$ with $w_0, \dots, w_r \in \mathcal{A} := \{0, 1, \dots, p-1\}$ and $w_r \neq 0$. The largest element of $L_{w_0}^{-1}(S)$ is $[w_r \cdots w_1]_p$. Continuing in this way we say that $\mathcal{V}_S$ contains a set whose largest element is $[w_r \cdots w_s]_p$ for $s = 0, 1, \dots, r$. The set $\mathcal{V}_S$ also contains $\{0\}$ and $\emptyset$. So we have $\operatorname{comp}_p(S) = |\mathcal{V}_S| \geq r + 3$. On the other hand, $m < p^{r+1}$. We have

$$m < p^{r+1} = p^{(r+3)-2} \leq p^{\operatorname{comp}_p(S)-2}.$$

□

Lemma 6.3. *Suppose that $S \subseteq \mathbb{N}$ is p-automatic and nonempty. If $m \in S$ is the smallest element, then $m < p^{\operatorname{comp}_p(S)-2}$.*

Proof. The proof goes the same as for the previous lemma. □

Lemma 6.4. *Suppose that $S_1, S_2 \subseteq \mathbb{N}$ are both p-automatic. Then we have*

$$\operatorname{comp}_p((S_1 \setminus S_2) \cup (S_2 \setminus S_1)) \leq \operatorname{comp}_p(S_1) \operatorname{comp}_p(S_2).$$

Proof. Every element of $\mathcal{V}_{(S_1 \setminus S_2) \cup (S_2 \setminus S_1)}$ is of the form

$$(U_1 \setminus U_2) \cup (U_2 \setminus U_1)$$

with $U_1 \in \mathcal{V}_{S_1}$ and $U_2 \in \mathcal{V}_{S_2}$. □

Similar proofs show that

$$\operatorname{comp}_p(S_1 \cap S_2) \leq \operatorname{comp}_p(S_1) \operatorname{comp}_p(S_2),$$
$$\operatorname{comp}_p(S_1 \cup S_2) \leq \operatorname{comp}_p(S_1) \operatorname{comp}_p(S_2),$$

and so forth.

Proposition 6.5. *Suppose that $\alpha_1(x), \dots, \alpha_d(x), \beta_1(x), \dots, \beta_d(x) \in \mathbb{F}_q[x]$ where q is a power of the prime p and define $a \in \mathbb{F}_q[x]^{\mathbb{N}}$ by*

$$a(n) = \beta_1(x)\alpha_1(x)^n + \cdots + \beta_d(x)\alpha_d(x)^n.$$

Suppose that $k \geq 2$ such that $\deg(\alpha_i(x)) \leq k$ and $\deg(\beta_i(x)) \leq (p-1)k$ for all i. Then we have

$$\operatorname{comp}_p(\mathcal{Z}(a)) \leq q^{d^2 k^4 p^4}.$$

Proof. Let V be the space all polynomials of degree $\leq (p-1)k$. We choose W as in Proposition 5.2. We follow the proof of Proposition 5.2 to find W explicitly. Let $m := p$ and define $h_1, \dots, h_p$ by $h_i = x^{i-1}$. We get a decomposition

$$\mathbb{F}_q[x] = \mathbb{F}_q[x]^{\langle p \rangle} h_1 \oplus \cdots \oplus \mathbb{F}_q[x]^{\langle p \rangle} h_p.$$

Note that $\mathbb{F}_q[x]^{\langle p\rangle} = \mathbb{F}_q[x^p]$. Let $n = \dim_{\mathbb{F}_q} V = k(p-1)+1$. We need to choose C such that

$$V^{n(p-1)} \subseteq (V^C)^{\langle p\rangle} h_1 \oplus \cdots \oplus (V^C)^{\langle p\rangle} h_p. \tag{16}$$

Now $V^{n(p-1)}$ is the set of all polynomials of degree $\leq n(p-1)^2 k$ and

$$(V^C)^{\langle p\rangle} h_1 \oplus \cdots \oplus (V^C)^{\langle p\rangle} h_p$$

is the set of all polynomials of degree at most $Cpk(p-1)+(p-1)$. It suffices that

$$n(p-1)^2 k \leq Cpk(p-1)+(p-1)$$

which is equivalent to

$$n(p-1)k \leq Cpk+1$$

and (because $k \geq 2$) to

$$n \leq \frac{Cp}{p-1}.$$

We take $C = \lceil n(p-1)/p \rceil$, so that

$$\begin{aligned} \frac{Cp}{p-1} &\leq \frac{n(p-1)+(p-1)}{p} = \frac{(n+1)(p-1)}{p} \\ &= \frac{((p-1)k+2)(p-1)}{p} < \frac{k(p+1)(p-1)}{p} < kp. \end{aligned} \tag{17}$$

In the proof of Proposition 5.2 we must take l such that $l > Cp/(p-1)$. So we may take $l = kp$ by (17). Define $W = V^{l-1} = V^{kp-1}$ which is the set of polynomials of degree $\leq (kp-1)k(p-1)$. We have $\dim W = (kp-1)k(p-1)+1 \leq k^2p^2$.

For U as in the proof of Theorem 4.14 we have

$$u := \dim U \leq d \cdot \dim W = dk^2p^2.$$

Let $\mathcal{W}$ be the collection of sets

$$\mathcal{Z}(b_1) \cap \cdots \cap \mathcal{Z}(b_r) \tag{18}$$

where $r \in \mathbb{N}$ and $b_1, \ldots, b_r \in U$. Note that (18) only depends on the $\mathbb{F}_q$-vector space spanned by $b_1, \ldots, b_r$. Therefore $|\mathcal{W}|$ is bounded by the number of subspaces of U. Every subspace of U can be generated by a $u \times u$ matrix with entries in $\mathbb{F}_q$. So a (rough) upper bound for the number of subspaces of U is

$$q^{u^2} \leq q^{d^2k^4p^4}.$$

We conclude that

$$|\mathcal{V}_{\mathcal{Z}(a)}| \leq |\mathcal{W}| \leq q^{d^2k^4p^4}.$$

□

Corollary 6.6. *In the setup of Proposition 6.5, we have then*

$$\min(\mathcal{Z}(a)) < p^{q^{d^2k^4p^4}}.$$

Proof. This follows from Proposition 6.5 and Lemma 6.3. □

Corollary 6.7. *In the setup of Proposition 6.5, if $\mathcal{Z}(a)$ is finite, then*

$$\max(\mathcal{Z}(a)) < p^{q^{d^2k^4p^4}}.$$

Proof. This follows from Proposition 6.5 and Lemma 6.2. □

Proposition 6.8. *Suppose that K is a finitely generated field over $\mathbb{F}_p$ and $a \in K^{\mathbb{N}}$ is a K-recurrence sequence which is simple and nondegenerate. (Assume that the recurrence relation is explicitly known.) One can compute an explicit bound $N(a)$ such that*

$$\operatorname{comp}_p(\mathcal{Z}(a)) \leq N(a).$$

Proof. By possibly enlarging the field K we can explicitly write

$$a(n) = \beta_1\alpha_1^n + \cdots + \beta_d\alpha_d^n,$$

where $\alpha_1, \ldots, \alpha_d, \beta_1, \ldots, \beta_d \in K$. As in the proof of Proposition 6.5, we can follow the proofs of Proposition 5.2 and Theorem 4.14 to find an explicit bound for $N(a)$. □

Proof of Theorem 1.10. We can reduce to the case where a is simple and nondegenerate by Lemma 2.4. It is possible to explicitly enumerate all p-normal sets $S_1, S_2, \ldots$. We can verify whether $\mathcal{Z}(a) = S_i$ as follows. Proposition 6.8 gives an upper bound for $\operatorname{comp}_p(\mathcal{Z}(a))$. One can explicitly construct an automaton that produces S_i reversely. This gives an upper bound $\operatorname{comp}_p(S_i)$. Let

$$U_i = (\mathcal{Z}(a) \setminus S_i) \cup (S_i \setminus \mathcal{Z}(a)).$$

Then $\operatorname{comp}_p(U_i) \leq \operatorname{comp}_p(\mathcal{Z}(a)) \operatorname{comp}_p(S_i)$ by Lemma 6.4, so we have an explicit upper bound for $\operatorname{comp}_p(U_i)$, say $\operatorname{comp}_p(U_i) \leq N$. If U_i is nonempty then the smallest element of U_i is at most p^{N-2} (see Lemma 6.3). So we have that $S_i = \mathcal{Z}(a)$ if and only if

$$S_i \cap \{0, 1, 2, \ldots, p^{N-2}\} = \mathcal{Z}(a) \cap \{0, 1, 2, \ldots, p^{N-2}\}$$

and this can be verified in a finite amount of time. □

7. Automata producing zero sets

For any simple nondegenerate linear recurrence sequence $a \in K^{\mathbb{N}}$ where K is a field of characteristic $p > 0$ we constructed a p-automaton that produces $\mathcal{Z}(a)$ reversely. In this section we will study how such an automaton can look like. As it turns out, these automata have a very special form.

Definition 7.1. Suppose that $S \subseteq \mathbb{N}$ is of the form $\mathcal{Z}(a)$ for some simple nondegenerate recurrence sequence $a \in K^{\mathbb{N}}$ where K is a field of characteristic $p > 0$. We define the *level* $\ell(S)$ of S as the smallest nonnegative integer d for which we can write

$$S = \mathcal{Z}(b_1) \cap \cdots \cap \mathcal{Z}(b_r),$$

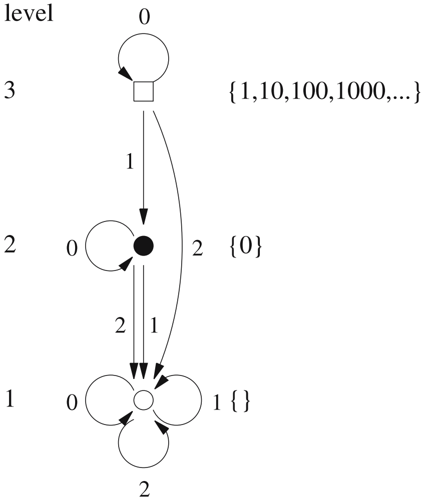
where $b_1, \ldots, b_r \in K^{\mathbb{N}}$ are linear recurrence sequences of order $\leq d$.

For example $\ell(\mathbb{N}) = 0$ because the zero sequence has minimum polynomial 1. Also $\ell(\emptyset) = 1$ because the sequence that is constant 1 has minimum polynomial $X - 1$. If $S \neq \emptyset, \mathbb{N}$ then $\ell(S) \geq 2$ because any linear recurrence sequence of order 1 is constant.

Example 7.2. Let $a \in \mathbb{F}_3(x)^{\mathbb{N}}$ be defined by

$$a(n) = (x+1)^n - x^n - 1$$

(See Example 1.3). The automaton producing $\mathcal{Z}(a) = \{1, 3, 9, 27, \ldots\}$ reversely is:

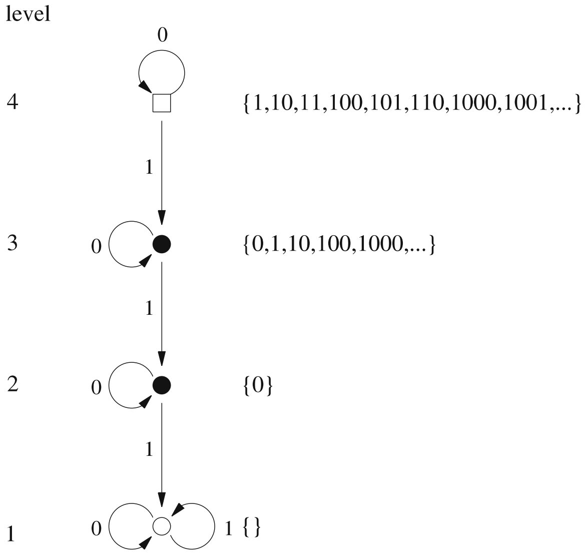


(elements in $\mathbb{N}$ are written in base 3).

Example 7.3. Let $a \in \mathbb{F}_2(x, y, z)^{\mathbb{N}}$ be defined by

$$a(n) = (x+y+z)^n - (x+y)^n - (x+z)^n - (y+z)^n + x^n + y^n + z^n$$

(See Proposition 3.2). The automaton producing $\mathcal{Z}(a) = \{2^i + 2^j | i, j \in \mathbb{N}\} \cup \{1\}$ reversely is:

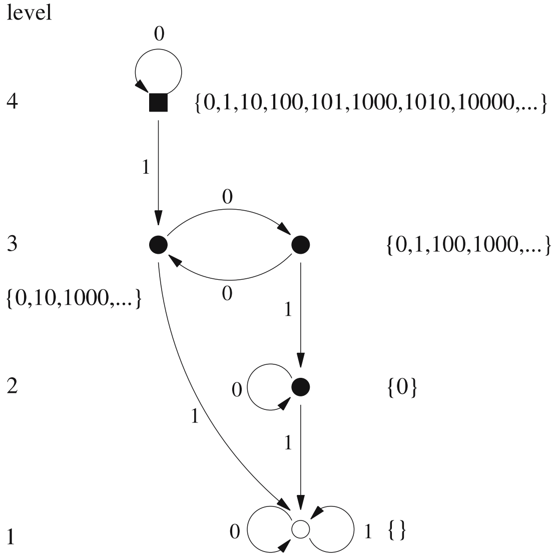


(in base 2).

Example 7.4. Let $a \in \mathbb{F}_4(x)^{\mathbb{N}}$ be defined by

$$a(n) = x^n + (x+1)^n + (x+\alpha)^n + (x+1+\alpha)^n$$

as in Example 3.4. The automaton producing $\mathcal{Z}(a)$ reversely is:



(in base 2).

Proposition 7.5. *Suppose that a is a simple nondegenerate nonzero recurrence sequence of order d in a field K of characteristic $p > 0$. Consider the automaton that produces $S = \mathcal{Z}(a)$ reversely and its graph.*

(a) *If $Q, R \in \mathcal{V}_S$ and there is a path from Q to R then $\ell(Q) \geq \ell(R)$.*
(b) *If $Q, R \in \mathcal{V}_S$ with $\ell(Q) \geq 2$ and there are two distinct paths from Q to R of the same length, then $\ell(Q) > \ell(R)$.*
(c) *$\mathbb{N} \notin \mathcal{V}_S$.*
(d) *$\emptyset \in \mathcal{V}_S$.*

Proof. (a) Suppose that $R = (L_i^p)^{-1}(Q)$ and that

$$Q = \bigcap_{j=1}^{r} \mathcal{Z}(b_j),$$

where b_j is a simple nondegenerate recurrence sequence of order $\leq \ell(Q)$ for all j. Then

$$R = \bigcap_{j=1}^{r} \mathcal{Z}\big(T_i^p b_j\big)$$

and $T_i^p b_j$ has order $\leq \ell(Q)$ for all j by Lemma 2.1. It follows that $\ell(R) \leq \ell(Q)$.

(b) Suppose that there are 2 paths from Q to R of length r. We can write

$$Q = \mathcal{Z}(a_1) \cap \cdots \cap \mathcal{Z}(a_s),$$

where a_i is a simple nondegenerate recurrence sequence of order at most $d := \ell(Q)$. Since there are two paths of length r from Q to R, we have

$$\big(L_j^{p^r}\big)^{-1}(Q) = R = \big(L_k^{p^r}\big)^{-1}(Q)$$

for some j, k with $0 \leq j < k < p^r$. This implies

$$R = \bigcap_{i=1}^{r} \mathcal{Z}\big(T_j^{p^r} a_i\big)$$

and

$$R = \bigcap_{i=1}^{r} \mathcal{Z}\big(T_k^{p^r} a_i\big)$$

By Lemma 7.6 below we can write

$$\mathcal{Z}\big(T_j^{p^r} a_i\big) \cap \mathcal{Z}\big(T_k^{p^r} a_i\big) = \mathcal{Z}(b_i) \cap \mathcal{Z}(c_i)$$

for certain recurrence sequences b_i and c_i of order $\leq d-1$. We see that

$$R = \bigcap_{i=1}^{r} \big(\mathcal{Z}\big(T_j^{p^r} a_i\big) \cap \mathcal{Z}\big(T_k^{p^r} a_i\big)\big) = \bigcap_{i=1}^{r} (\mathcal{Z}(b_i) \cap \mathcal{Z}(c_i)).$$

It follows that $\ell(R) \leq d-1 < \ell(Q)$.

(c) For every $Q \in \mathcal{V}_S$ there exists an r and j such that $Q = \mathcal{Z}(T_j^{p^r} a)$. Since a is simple and nondegenerate, $T_j^{p^r} a$ cannot be the 0 sequence by Lemma 2.6.

(d) Let $Q \in \mathcal{V}_S$ with $\ell(Q)$ minimal. There are p^r paths starting at Q of length r. Choose r such that $p^r > |\mathcal{V}_S|$. By the pigeonhole principle, there are two paths of length r which have the same endpoint, say R. If $\ell(Q) \geq 2$ then $\ell(Q) > \ell(R)$ by part (b) and we have a contradiction. Therefore, $\ell(Q) \leq 1$, so $Q = \emptyset$ or $Q = \mathbb{N}$. But $Q \neq \mathbb{N}$ by part (c). □

Lemma 7.6. *Suppose that $a \in K^{\mathbb{N}}$ is a simple and nondegenerate sequence of order $d \geq 2$ where K is a field of characteristic $p > 0$. If $j \neq k$ then there exist simple and nondegenerate sequences $b, c \in K^{\mathbb{N}}$ of order $\leq d-1$ such that*

$$\mathcal{Z}\big(T_j^{p^r} a\big) \cap \mathcal{Z}\big(T_k^{p^r} a\big) = \mathcal{Z}(b) \cap \mathcal{Z}(c).$$

Proof. We can write

$$a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^n.$$

We have

$$\big(T_j^{p^r} a\big)(n) = \sum_{i=1}^{d} \big(\beta_i \alpha_i^j\big)\big(\alpha_i^{p^r}\big)^n$$

(and a similar formula for $T_k^{p^r} a$). Define

$$b = \alpha_1^k T_j^{p^r} a - \alpha_1^j T_k^{p^r} a$$

and

$$c = \alpha_2^k T_j^{p^r} a - T_j^{p^r} \alpha_2^j T_k^{p^r} a.$$

By construction, the coefficient of $(\alpha_1^{p^r})^n$ in $b(n)$ vanishes. Similarly, the coefficient of $(\alpha_2^{p^r})^n$ in $c(n)$ vanishes. This shows that b and c have order $\leq d-1$. Since α_1/α_2 is not a root of unity, we have

$$\det \begin{pmatrix} \alpha_1^k & -\alpha_1^j \\ \alpha_2^k & -\alpha_2^j \end{pmatrix} \neq 0.$$

Therefore, the K-span of b and c is the same as the span of $T_k^{p^r}a$ and $T_j^{p^r}a$, hence

$$\mathcal{Z}\big(T_j^{p^r}a\big) \cap \mathcal{Z}\big(T_k^{p^r}a\big) = \mathcal{Z}(b) \cap \mathcal{Z}(c).$$

□

Definition 7.7. Let $\mathcal{A} = \{0, 1, \ldots, p-1\}$. Suppose that $u_0, u_1, \ldots, u_d$, $w_1, \ldots, w_d \in \mathcal{A}^\star$. We define

$$\begin{aligned} &U_p(u_0, u_1, \ldots, u_d; w_1, \ldots, w_d) \\ &\qquad = \big\{\big[u_d w_d^{k_d} u_{d-1} w_{d-1}^{k_{d-1}} \cdots u_1 w_1^{k_1} u_0\big]_p \big| k_1, k_2, \ldots, k_d \in \mathbb{N}\big\} \subseteq \mathbb{N}. \end{aligned}$$

Proposition 7.8. *Let $a \in K^{\mathbb{N}}$ be a nonzero, simple and nondegenerate sequence of order d, where K is a field of characteristic $p > 0$. Then $S := \mathcal{Z}(a)$ is a finite union of sets of the form $U_p(u_0, \ldots, u_m; w_1, \ldots, w_m)$ with $m \leq d - 2$.*

Proof. Consider the graph with vertex set $\mathcal{V}_S$ of the automaton that produces S reversely. We let words act on the left using the convention (10). If $w = i_r i_{r-1} \cdots i_0$ then the path given by the word w starting at some vertex Q is the path in the graph that visits the vertices

$$Q, i_0 \cdot Q, i_1 i_0 \cdot Q, \ldots, i_r i_{r-1} \cdots i_0 \cdot Q.$$

A vertex Q in $\mathcal{V}_S$ is called a *loop vertex* if there is a nontrivial path from Q to itself. In other words, Q is a loop vertex if and only if $w \cdot Q = Q$ for some nontrivial word w. Let us choose w nontrivial of minimal length such that $w \cdot Q = Q$. Then the path from Q to Q via w does not intersect itself (except at the beginning and the end). We claim that every path from Q to Q is given by a power of w. Suppose that $u \cdot Q = Q$. We can write $u = yw^s$ where y is a path that does not have w as a suffix, i.e., y is not of the form zw for some word z. If y is the trivial path then were are done, so assume to the contrary that y is not trivial. Let e and f be the lengths of w and y respectively. Then y^e and w^f are paths from Q to Q of length ef. Since tautologically $\ell(Q) = \ell(Q)$, we have $y^e = w^f$ by Proposition 7.5(b). Since $e \leq f$, w has to be a suffix of y. Contradiction. We conclude that every loop from Q to Q is given by a power of w.

Suppose that $n \in S$. We can write $n = [w]_p$ for some word w. Consider the path γ from S to $Q := w \cdot S$ given by w. Define $S_0, S_1, S_2, \ldots$ as follows. First we define $S_0 = S$. For $j > 0$ we define S_j as the first loop vertex in the path γ from which there exists no path to S_{j-1} if such a vertex exists. Suppose that we can define $S_1, S_2, \ldots, S_m$ in this way. We define $S_{m+1} = Q$. We can write

$$w = u_m w_m^{l_m} u_{m-1} w_{m-1}^{l_{m-1}} u_{m-2} \cdots u_1 w_1^{l_1} u_0,$$

where u_j defines a path from S_j to S_{j+1} without self-intersection, w_j defines the unique nontrivial loop at vertex S_j without self intersection, and $l_j \in \mathbb{N}$ for all j.

For j with $1 \leq j < m$, for every i, k we have that

$$w_{j+1}^{l} u_j w_j^{k}$$

defines a path from S_j to S_{j+1}. Let s_j and s_{j+1} be the lengths of w_j and w_{j+1} respectively. Then $w_{j+1}^{s_j} u_j$ and $u_j w_j^{s_{j+1}}$ define paths from S_j to S_{j+1} of equal length. Since $w_{j+1}^{s_j} u_j$ visits vertex S_j only once at the beginning, and $u_j w_j^{s_{j+1}}$ visits S_j exactly $s_{j+1} + 1$ times, we have that $w_{j+1}^{s_j} u_j \neq u_j w_j^{s_{j+1}}$. From Proposition 7.5(b) it follows that $\ell(S_{j+1}) > \ell(S_j)$.

We deduce that S contains $U_p(u_0, u_1, \ldots, u_m; w_1, \ldots, w_m)$. Note that

$$\begin{aligned} d \geq \ell(S) = \ell(S_0) > \ell(S_1) > \ell(S_2) > \cdots > \ell(S_m) \\ \geq \ell(S_{m+1}) = \ell(Q) \geq 2. \end{aligned}$$

It follows that $m \leq d - 2$.

Since there are only finitely many paths without self-intersection and only finitely many loops without self-intersection, it follows that S is a finite union of sets of the form $U_p(u_0, u_1, \ldots, u_m; w_1, \ldots, w_m)$ with $m \leq d - 2$. □

8. Proof of the main result

In this section we will prove Theorem 2.7. This also completes the proof of Theorem 1.8.

Lemma 8.1. *Suppose that $a \in K^{\mathbb{N}}$ is a simple nondegenerate sequence in a field K of characteristic $p > 0$. Suppose that q is a power of p and that $r, s \in \mathbb{Q}$. If*

$$\{r + sq^n | n \geq m\} \subseteq \mathcal{Z}(a)$$

for some constant $m \in \mathbb{N}$ then

$$\{r + sq^n | n \in \mathbb{N}\} \cap \mathbb{N} \subseteq \mathcal{Z}(a).$$

Proof. We can write

$$a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^n$$

where α_i/α_j is not a root of unity for all $i \neq j$. Choose $N \in \mathbb{N}$ such that $Nr, Ns \in \mathbb{Z}$. Choose λ_i such that $\lambda_i^N = \alpha_i$. Then λ_i/λ_j is not a root of unity for $i \neq j$ and

$$b(n) = \sum_{i=1}^{d} \beta_i \lambda_i^n$$

is a simple nondegenerate sequence with $b(Nn) = a(n)$ and

$$b(Nr + (Ns)q^n) = a(r + sq^n).$$

The sequence $c(n)$ defined by

$$c(n) = b(Nr + (Ns)n) = a(r + sn)$$

is also a simple nondegenerate sequence. So we can reduce the lemma to the case that $r = 0$ and $s = 1$.

Let us assume that

$$a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^n.$$

is a simple nondegenerate sequence with $a(q^n) = 0$ for $n \geq m$. We will show that $a(q^n) = 0$ for all $n \in \mathbb{N}$. Consider the element

$$x = \sum_{i=1}^{d} \beta_i \otimes \alpha_i \in K \otimes_{\mathbb{F}_q} K.$$

Suppose that $x \neq 0$. Let us write

$$x = \sum_{i=1}^{e} \delta_i \otimes \gamma_i,$$

where e is minimal. This implies that $\gamma_1, \dots, \gamma_e$ are linearly independent over $\mathbb{F}_q$. Similarly, $\delta_1, \dots, \delta_e$ are linearly independent over $\mathbb{F}_q$. Let $\phi : K \to K$ be the Frobenius homomorphism defined by $\phi(\epsilon) = \epsilon^q$. The homomorphism ϕ leaves the field $\mathbb{F}_q$ invariant. Define $\psi : K \otimes_{\mathbb{F}_q} K \to K$ by $\psi(\sum_i \lambda_i \otimes \nu_i) = \sum_i \lambda_i \nu_i$. We have

$$\psi \circ (\mathrm{id} \otimes \phi^n)\Big(\sum_{i=1}^{d} \beta_i \otimes \alpha_i\Big) = \psi\Big(\sum_{i=1}^{d} \beta_i \otimes \alpha_i^{q^n}\Big) = \sum_{i=1}^{d} \beta_i \alpha_i^{q^n} = a(q^n).$$

By assumption this is equal to 0 for $n \geq m$. On the other hand, this is equal to

$$\begin{aligned}\psi \circ (\mathrm{id} \otimes \phi^n)\Big(\sum_{i=1}^{e} \delta_i \otimes \gamma_i\Big) &= \psi\Big(\sum_{i=1}^{e} \delta_i \otimes \gamma_i^{q^n}\Big) \\ &= \sum_{i=1}^{e} \delta_i \otimes \gamma_i^{q^n} = \sum_{i=1}^{e} \delta_i \gamma_i^{q^n}.\end{aligned}$$

Define $c_1, \dots, c_e \in K^{\mathbb{N}}$ by

$$c_j(n) = \gamma_j^{q^n}.$$

We know that $E^m c_1, \dots, E^m c_e$ are linearly dependent over K because

$$\left(\sum_{j=1}^{e} \delta_j E^m c_j\right)(n) = \sum_{j=1}^{e} \delta_j \gamma_j^{q^{m+n}} = a(q^{n+m}) = 0$$

for all $n \in \mathbb{N}$. Choose j maximal such that $E^n c_1, \dots, E^n c_{j-1}$ are linearly independent for all $n \in \mathbb{N}$. Then $E^n c_1, \dots, E^n c_j$ are linearly dependent for n large enough. There are unique $\epsilon_1, \dots, \epsilon_{j-1} \in K$ such that

$$E^n c_j = \sum_{i=1}^{j-1} \epsilon_i E^n c_i. \tag{19}$$

Taking the q-th power of (19) yields:

$$E^{n+1} c_j = \left(E^n c_j\right)^q = \sum_{i=1}^{j-1} \epsilon_i^q \left(E^n c_i\right)^q = \sum_{i=1}^{j-1} \epsilon_i^q E^{n+1} c_i. \tag{20}$$

Applying E to (19) yields:

$$E^{n+1} c_j = \sum_{i=1}^{j-1} \epsilon_i E^{n+1} c_i. \tag{21}$$

Subtracting (21) from (20) gives:

$$0 = \sum_{i=1}^{j-1} \left(\epsilon_i^q - \epsilon_i\right) E^{n+1} c_i$$

Since $E^{n+1} c_1, E^{n+1} c_2, \dots, E^{n+1} c_{j-1}$ are linearly independent over K, we conclude that

$$\epsilon_i^q = \epsilon_i$$

for $i = 1, 2, \dots, j-1$. This means that $\epsilon_1, \dots, \epsilon_{j-1} \in \mathbb{F}_q$. Therefore

$$E^n c_1 = c_1^{q^n}, \dots, E^n c_j = c_j^{q^n}$$

are linearly dependent over $\mathbb{F}_q$. Taking the q^n-th root shows us that $c_1, \dots, c_j$ are linearly dependent over $\mathbb{F}_q$. But then $\gamma_1, \dots, \gamma_j$ are linearly dependent over $\mathbb{F}_q$. Contradiction! We conclude that $x = 0$. It follows that $a(q^n) = 0$ for all n. □

Proof of Theorem 2.7. By Proposition 7.8, $\mathcal{Z}(a)$ is a finite union of sets of the form $U_p(u_0, u_1, \dots, u_m; w_1, \dots, w_m)$ with $m \leq d-2$. Let r_i be the length of w_i and let r be the least common multiple of $r_1, \dots, r_m$. We can write $U_p(u_0, \dots, u_m; w_1, \dots, w_m)$ as a finite union of sets of the form

$$U_p\bigl(u'_0, \dots, u'_m; w_1^{k_1}, \dots, w_m^{k_m}\bigr),$$

where $k_i = r/r_i$. This shows that $\mathcal{Z}(a)$ is a finite union of sets of the form

$$U_p(u_0, u_1, \dots, u_m; w_1, \dots, w_m)$$

where $w_1, \dots, w_m$ all have the same length r. Set $q = p^r$ and let t_i be the length of u_i for all i. From

$$\begin{aligned}\bigl[u_m w_m^{k_m} u_{m-1} w_{m-1}^{k_{m-1}} \cdots u_1 w_1^{k_1} u_0\bigr]_p \\ &= \sum_{i=0}^{m} [u_i]_p p^{t_0+t_1+\cdots+t_{i-1}} q^{k_1+k_2+\cdots+k_i} \\ &\quad + \sum_{i=1}^{m} [w_i]_p p^{t_0+t_1+\cdots+t_{i-1}} q^{k_1+\cdots+k_{i-1}} \left(\frac{q^{k_i}-1}{q-1}\right)\end{aligned}$$

it follows that the set $U_q(u_0, \dots, u_m; w_1, \dots, w_m)$ has the form

$$\bigl\{c_0 + c_1 q^{l_1} + c_2 q^{l_2} + \cdots + c_r q^{l_m} \bigm| 0 \leq l_1 \leq l_2 \leq \cdots \leq l_m\bigr\} \tag{22}$$

with $c_0, c_1, \dots, c_m \in \mathbb{Q}$ such that $c_0 + \cdots + c_m \in \mathbb{Z}$ and $(q-1)c_i \in \mathbb{Z}$ for all i. We will show that $\mathcal{Z}(a)$ contains

$$\bigl\{c_0 + c_1 q^{l_1} + c_2 q^{l_2} + \cdots + c_m q^{l_m} \bigm| l_1, \dots, l_m \in \mathbb{N}\bigr\} \cap \mathbb{N},$$

where it is not required anymore that the sequence $l_0, \dots, l_m$ be non-decreasing. Suppose that $l_1, \dots, l_m \in \mathbb{N}$ such that

$$c_0 + c_1 q^{l_1} + c_2 q^{l_2} + \cdots + c_m q^{l_m} \in \mathbb{N}.$$

We would like to show that

$$c_0 + c_1 q^{l_1} + c_2 q^{l_2} + \cdots + c_m q^{l_m} \in \mathcal{Z}(a).$$

Since $c_m > 0$, it suffices to show, by Lemma 8.1, that

$$c_0 + c_1 q^{l_1} + c_2 q^{l_2} + \cdots + c_{m-1} q^{l_{m-1}} + c_m q^{l_m+N} \in \mathcal{Z}(a)$$

for $N \gg 0$. We prove this by induction on

$$D := |\{i | 1 \leq i \leq m-1, l_i > l_{i+1}\}|.$$

The case $D = 0$ follows from (22). If $D > 0$, then there exists an i such that $l_i > l_{i+1}$. For N sufficiently large we have

$$c_{i+1}q^{l_{i+1}} + c_{i+2}q^{l_{i+2}} + \cdots + c_{m-1}q^{l_{m-1}} + c_m q^{l_m+N} > 0.$$

For $M \geq l_i - l_{i+1}$ we get

$$\left(c_1q^{l_1} + \cdots + c_iq^{l_i}\right) \\ + \left(c_{i+1}q^{l_{i+1}+M} + \cdots + c_{m-1}q^{l_{m-1}+M} + c_mq^{l_m+M+N}\right) \in \mathcal{Z}(a)$$

by induction. From Lemma 8.1 it follows that

$$c_0 + c_1q^{l_1} + c_2q^{l_2} + \cdots + c_{m-1}q^{l_{m-1}} + c_mq^{l_m+N} \in \mathcal{Z}(a)$$

and we are done. □

We remark that Theorem 2.7 is related to the following theorem of Masser (see [18], [24, §28] and [12, page 707]).

Theorem 8.2. *Let K be a field of characteristic $p > 0$ with algebraic closure $\overline{K} \supseteq K$, $d \geq 1$ and let $\alpha_1, \ldots, \alpha_d \in K \setminus \{0\}$. The following conditions are equivalent:*

(1) *There exist $\beta_1, \ldots, \beta_d \in K$ such that*

$$\beta_1\alpha_1^n + \cdots + \beta_n\alpha_d^n = 0$$

for infinitely many $n \in \mathbb{N}$;

(2) *There exist positive integers $u, v \in \mathbb{N}$ and $\gamma_1, \ldots, \gamma_d \in \overline{K}$ such that $\alpha_i = \gamma_i^u$ for all i and $\gamma_1^v, \ldots, \gamma_d^v$ are linearly dependent over $\overline{\mathbb{F}}_p$;*

(3) *If $L = K \cap \overline{\mathbb{F}}_p$, then there exist positive integers u, v and elements $\mu_1, \ldots, \mu_d \in L$ and $\gamma_1, \ldots, \gamma_d \in \overline{K}$, such that $\alpha_i = \mu_i\gamma_i^u$ for all i and $\gamma_1^v, \ldots, \gamma_d^v$ are linearly dependent over L.*

For example, the implication (1) ⇒ (2) follows from the results in this paper as follows. Suppose that

$$a(n) = \beta_1\alpha_1^n + \cdots + \beta_n\alpha_d^n$$

satisfies $a(n) = 0$ for infinitely many n. If a is not nondegenerate, then α_i/α_j is a root of unity for some $i \neq j$, say $(\alpha_i/\alpha_j)^N = 1$. Then clearly we may take $u = 1$ and $v = N$ and $\gamma_i = \alpha_i$ for all i. Thus, suppose that $a(n)$ is nondegenerate. By Theorem 2.7 there exist r, $s \in \mathbb{N}$ and p-power q such that $a(r+sq^n) = 0$ for all n. If we follow the proof of Lemma 8.1 then (2) follows. (In particular $x = 0$ implies that $\alpha_1, \ldots, \alpha_d$ are linearly dependent over $\mathbb{F}_q$).

It may be possible to use Masser's theorem to prove some of the results in this paper.

9. Recurrence sequences in modules

In this section we will study recurrence sequences in modules over arbitrary commutative algebras. Our main goal is to prove Theorem 1.2 and Theorem 1.9. First we prove that the intersection of two p-normal sets is again p-normal.

Definition 9.1. A subset $N \subseteq \mathbb{Z}^r$ is called a *rectangular coset in* $\mathbb{Z}^r$ if it is of the form

$$N = e_0 + e_1\mathbb{Z} + e_2\mathbb{Z} + \cdots + e_s\mathbb{Z},$$

where $e_0, e_1, e_2, \ldots, e_s \in \mathbb{Z}^r$ and $e_1, \ldots, e_s$ are pairwise orthogonal nonzero idempotent elements in $\mathbb{Z}^r$.

Note that idempotent vectors in $\mathbb{Z}^r$ consist of 0's and 1's. If e_i and e_j are orthogonal (i.e., $e_ie_j = 0$), then there is no position where e_i and e_j both have a 1.

Definition 9.2. We call $N \subseteq \mathbb{N}^r$ a *rectangular coset in* $\mathbb{N}^r$ if it is of the form

$$N = e_0 + e_1\mathbb{N} + \cdots + e_s\mathbb{N}$$

where $e_0, \ldots, e_s \in \mathbb{N}^r$ and $e_1, \ldots, e_s$ are pairwise orthogonal nonzero idempotents.

Lemma 9.3. *Suppose that $c_1, \ldots, c_r \in \mathbb{Q} \setminus \{0\}$ and $q \in \mathbb{Q}$ with $q > 1$. The set*

$$A = \left\{(l_1, \ldots, l_r) \in \mathbb{Z}^r \middle| c_1q^{l_1} + \cdots + c_rq^{l_r} = 0\right\}$$

is a finite union of rectangular cosets in $\mathbb{Z}^r$.

Proof. We prove this lemma by induction on r. The case $r = 1$ is clear. Choose $D \in \mathbb{N}$ such that

$$\left|c_iq^D\right| > \sum_{j \neq i} |c_j| \tag{23}$$

for all i.

We claim that for every $(l_1, \ldots, l_r) \in A$ there exist distinct indices i and j such that $l_j \leq l_i \leq D + l_j$. Take i such that l_i is maximal. Suppose that $l_i > D + l_j$ for all $j \neq i$. Then we get

$$0 = \sum_{j=1}^{r} c_jq^{l_j},$$

so

$$|c_i|q^{l_i} = \left|c_iq^{l_i}\right| = \left|\sum_{j \neq i} c_jq^{l_j}\right| \leq \sum_{j \neq i} \left|c_jq^{l_j}\right| \leq \sum_{j \neq i} |c_j|q^{l_i - D}$$

and

$$|c_i|q^D > \sum_{j\neq i}|c_j|.$$

This is in contradiction with (23). Therefore, $l_i \leq D + l_j$ for some $j \neq i$.

We can write

$$A = \bigcup_{i\neq j}\bigcup_{k=0}^{D} A_{i,j,k},$$

where

$$A_{i,j,k} = A \cap \{(l_1, \ldots, l_r)|l_i = l_j + k\}.$$

Define

$$\begin{aligned} B_{i,j,k} = \Big\{(l_1, \ldots, l_{i-1}, l_{i+1}, \ldots, l_r) \in \mathbb{Z}^r \Big| \\ c_1q^{l_1} + \cdots + c_{i-1}q^{l_{i-1}} + c_{i+1}q^{l_{i+1}} + \cdots \\ + (c_iq^k + c_j)q^{l_j} + \cdots + c_rq^{l_r} = 0\Big\}, \end{aligned}$$

so that

$$\begin{aligned} A_{i,j,k} = \Big\{(l_1, \ldots, l_{i-1}, l_j + k, l_{i+1}, \ldots, l_r) \in \mathbb{Z}^{r-1}\Big| \\ (l_1, \ldots, l_{i-1}, l_{i+1}, \ldots, l_r) \in B_{i,j,k}\Big\}. \end{aligned}$$

By the induction hypothesis, $B_{i,j,k}$ is a finite union of rectangular cosets. Therefore, $A_{i,j,k}$ is a finite union of rectangular cosets. We conclude that A is a finite union of rectangular cosets. □

We also have the following monoid version of this Lemma 9.3.

Corollary 9.4. *Suppose that $c_1, \ldots, c_r \in \mathbb{Q}$ are nonzero and $q \in \mathbb{Q}$ with $q > 1$. The set*

$$A = \Big\{(l_1, \ldots, l_r) \in \mathbb{N}^r \Big| c_1q^{l_1} + \cdots + c_rq^{l_r} = 0\Big\}$$

is a finite union of rectangular cosets of in $\mathbb{N}^r$.

Proof. This follows from the previous lemma and the observation that a rectangular coset in $\mathbb{Z}^r$ intersected with $\mathbb{N}^r$ is a rectangular coset in $\mathbb{N}^r$. □

Lemma 9.5. *Suppose that $S_1, S_2 \subseteq \mathbb{N}$. are both p-normal of order $\leq d$, then $S_1 \cap S_2$ is p-normal of order $\leq d$.*

Proof. Without loss of generality we may assume that S_1 is an infinite arithmetic progression or an elementary p-nested set of order $\leq d$. Similarly, we may assume that S_2 is an infinite arithmetic progression or an elementary p-nested set of order $\leq d$.

Case 1. The lemma is clear if both S_1 and S_2 are infinite arithmetic progressions.

Case 2. Suppose $S_1 = m + n\mathbb{N}$ is an infinite arithmetic progression and $S_2 = S_q(c_0; c_1, \dots, c_r)$ with $r \leq d$. Without loss of generality we may assume that $m < n$. Then we have $S_1 = (m + n\mathbb{Z}) \cap \mathbb{N}$. We can write $n = p^l u$ with $l \in \mathbb{N}$ and $\gcd(u, p) = \gcd(u, q) = 1$. Since $m + n\mathbb{N} = (m + p^l\mathbb{N}) \cap (m + u\mathbb{N})$ by the Chinese Remainder Theorem, we may assume that either $\gcd(n, q) = 1$ or n divides some power of q.

Case 2a. Suppose that $\gcd(n, q) = 1$. Choose s such that $q^s \equiv 1 \bmod n(q-1)$. There exists a decomposition

$$S_q(c_0; c_1, \dots, c_r) = \bigcup_{0 \leq l_1, \dots, l_r < s} S_{q^s}\big(c_0; c_1 q^{l_1}, \dots, c_r q^{l_r}\big).$$

There is an inclusion

$$S_{q^s}\big(c_0; c_1 q^{l_1}, \dots, c_r q^{l_r}\big) \subseteq c_0 + c_1 q^{l_1} + \cdots c_r q^{l_r} + n\mathbb{Z},$$

because $(q-1)c_i \in \mathbb{Z}$ for all i and $q^s \equiv 1 \bmod (q-1)n$. It follows that $S_1 \cap S_2 = S_q(c_0; c_1, \dots, c_r) \cap (m + n\mathbb{Z})$ is the union of all $S_{q^s}(c_0; c_1 q^{l_1}, \dots, c_r q^{l_r})$ for which

$$c_0 + c_1 q^{l_1} + \cdots + c_r q^{l_r} \equiv m \bmod n.$$

So $S_1 \cap S_2$ is p-normal of order $\leq d$.

Case 2b. Suppose that n divides q^s for some positive integer s. Then $S_q(c_0; c_1, \dots, c_r)$ is the union of all

$$S_q\big(c_0 + c_{i_1} q^{l_1} + \cdots + c_{i_u} q^{l_u}, c_{j_1} q^s, c_{j_2} q^s, \dots, c_{j_v} q^s\big)$$

for which $\{1, 2, \dots, r\}$ is a disjoint union of $\{i_1, \dots, i_u\}$ and $\{j_1, \dots, j_v\}$, $r = u + v$ and $0 \leq l_1, l_2, \dots, l_u < s$. Note that

$$\begin{aligned} S_q\big(c_0 + c_{u_1} q^{l_1} + \cdots + c_{i_u} q^{l_u}, c_{j_1} q^s, c_{j_2} q^s, \dots, c_{j_v} q^s\big) \\ \subseteq c_0 + c_{u_1} q^{l_1} + \cdots + c_{i_u} q^{l_u} + n\mathbb{Z}. \end{aligned}$$

because n divides q^s. We conclude that $S_1 \cap S_2$ is p-normal of order $\leq d$ as in Case 2a.

Case 3. Suppose that $S_1 = S_q(c_0; c_1, \dots, c_r)$ and $S_2 = S_{q'}(c'_0; c'_1, \dots, c'_{r'})$. If q'' is an integral power of q and also an integral power of q' then both S_1 and S_2 can be written as a finite union of sets of the form $S_{q''}(f_0; f_1, \dots, f_s)$. We can reduce to the case where $q' = q$.

The set

$$M = \{(l_1, \dots, l_r, l'_1, \dots, l'_{r'}) \in \mathbb{N}^{r+r'} | c_0 + c_1 q^{l_1} + \dots + c_r q^{l_r} = e_0 + e_1 q^{l'_1} + \dots + e_{r'} q^{l'_{r'}}\}$$

is a finite union of rectangular cosets (see Corollary 9.4). From this it follows that

$$\{(l_1, \dots, l_r) \in \mathbb{N}^r | \exists l'_1, \dots, l'_{r'} \in \mathbb{N} : c_0 + c_1 q^{l_1} + \dots + c_r q^{l_r} = e_0 + e_1 q^{l'_1} + \dots + e_{r'} q^{l'_{r'}}\}$$

is also a finite union of rectangular cosets in $\mathbb{N}^r$. Therefore

$$S_q(c_0; c_1, \dots, c_r) \cap S_q(c'_0; c'_1, \dots, c'_{r'})$$

is a finite union of sets of the form

$$S_q(f_0; f_1, \dots, f_u)$$

with $u \le r \le d$. This shows that

$$S_1 \cap S_2 = S_q(c_0; c_1, \dots, c_r) \cap S_q(c'_0; c'_1, \dots, c'_{r'})$$

is p-normal of order $\le d$. □

Suppose R is a commutative ring, M is an R-module and $\mathfrak{p} \subset R$ is a prime ideal. A submodule $N \subseteq M$ is called $\mathfrak{p}$-primary if $\mathfrak{p}$ is the only associated prime of M/N. We call M $\mathfrak{p}$-coprimary if the only associated prime of M is $\mathfrak{p}$ (i.e., if the submodule $(0) \subseteq M$ is $\mathfrak{p}$-primary). (See [4, §3.3])

Lemma 9.6. *Suppose that K is a field, R is a finitely generated K-algebra and M is a finitely generated R-module. If $a \in M^{\mathbb{N}}$ is an R-recurrence sequence of order d, then there exist prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_l \in R$, finitely generated R-modules $M_1, \dots, M_l$ where M_i is $\mathfrak{p}_i$-coprimary for all i and R-recurrence sequences $a_1, a_2, \dots, a_l$ of order $\le d$ with $a_i \in M_i^{\mathbb{N}}$ such that*

$$\mathcal{Z}(a) = \bigcap_{i=1}^{l} \mathcal{Z}(a_i).$$

Proof. We use the primary decomposition of M. There exist prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_l$ and submodules $N_1, N_2, \dots, N_l$ of M such that $\bigcap_{i=1}^{l} N_i = 0$ and N_i is a $\mathfrak{p}_i$-primary submodule of M for $i = 1, 2, \dots, l$ (see [4, Theorem 3.10]). Let $\rho_i : M \to M_i := M/N_i$ be the quotient homomorphism. Because the intersection of the kernels of $\rho_i, i = 1, 2, \dots, l$ is equal to 0, we get

$$\mathcal{Z}(a) = \bigcap_{i=1}^{l} \mathcal{Z}(\rho_i(a)).$$

Now take $a_i = \rho_i(a) \in M_i^{\mathbb{N}}$. □

Lemma 9.7. *Suppose that K is a field of characteristic p, R is a finitely generated domain over K and M is a finitely generated torsion-free R-module. Suppose that $a \in M^{\mathbb{N}}$ is an R-recurrence sequence of order d. If $p = 0$ then $\mathcal{Z}(a)$ is a union of a finite set and finitely many infinite arithmetic progressions. If $p > 0$, then $\mathcal{Z}(a)$ is p-normal of order $\leq d - 2$.*

Proof. Let L be the quotient field of R. We may view a as an L-recurrence sequence of order $\leq d$ in the vector space $V = M \otimes_R L \supseteq M$. Choose a basis $e_1, \dots, e_r$ of V. We can write $a = \sum_{i=1}^r a_i e_i$ with $a_i \in L^{\mathbb{N}}$ a L-recurrence sequence of order $\leq d$ for all i. We have

$$\mathcal{Z}(a) = \bigcap_{i=1}^{r} \mathcal{Z}(a_i).$$

If $p = 0$ then each $\mathcal{Z}(a_i)$ is a union of a finite set and finitely many arithmetic progressions by the Skolem–Mahler–Lech theorem (Theorem 1.1). Hence, $\mathcal{Z}(a)$ is a union of a finite set and finitely many infinite arithmetic progressions.

If $p > 0$, then $\mathcal{Z}(a_i)$ is p-normal of order $\leq d-2$ for all i by Theorem 1.8. This implies that $\mathcal{Z}(a)$ is p-normal of order $\leq d - 2$ by Lemma 9.5. □

Lemma 9.8. *Suppose that K is an infinite field of characteristic p, R is a finitely generated K-algebra, $\mathfrak{p} \subseteq R$ is a prime ideal, M is a finitely generated $\mathfrak{p}$-coprimary module, and $a \in M^{\mathbb{N}}$ is a linear R-recurrence sequence. If $p = 0$ then $\mathcal{Z}(a)$ is a union of a finite set and finitely arithmetic progressions. If $p > 0$ then $\mathcal{Z}(a)$ is p-normal.*

Proof. By the Noether Normalization Lemma (see for example [4, §8.2.1]), there exist algebraically independent $x_1, x_2, \dots, x_s \in R/\mathfrak{p}$ such that $R/\mathfrak{p}$ is a finitely generated $K[x_1, \dots, x_s]$-module. Choose $y_1, \dots, y_s \in R$ such that $y_i + \mathfrak{p} = x_i$ for all i.

Now M is also a $K[y_1, \dots, y_s]$-module. Since M is $\mathfrak{p}$-coprimary, there exists $t \in \mathbb{N}$ such that $\mathfrak{p}^t M = 0$ (see [4, Proposition 3.9]). We have a filtration

$$M \supseteq \mathfrak{p}M \supseteq \mathfrak{p}^2 M \supseteq \cdots \supseteq \mathfrak{p}^t M = 0$$

and each quotient $\mathfrak{p}^i M/\mathfrak{p}^{i+1} M$ is a finitely generated $R/\mathfrak{p}R$-module, hence a finite generated $K[y_1, \dots, y_s]$-module. It follows that M is a finitely generated $K[y_1, \dots, y_s]$-module. Similarly, $R/\mathfrak{p}^t R$ is a finitely generated $K[y_1, \dots, y_s]$-module. The R-module generated by $a, Ea, E^2a, \dots$ is finitely generated as an $R/\mathfrak{p}^t$-module, hence it is finitely generated as a $K[y_1, \dots, y_s]$-module. Therefore, a satisfies a $K[y_1, \dots, y_s]$-recurrence relation. However, the order of a as a $K[y_1, \dots, y_s]$-recurrence sequence can be larger than the order of a viewed as an R-recurrence sequence.

Since $\mathfrak{p} \cap K[y_1, \ldots, y_s] = (0)$, the annihilator in $K[y_1, \ldots, y_s]$ of any nonzero element in M is the zero ideal. We can reduce to the situation where $R = K[y_1, \ldots, y_s]$ is the polynomial ring and M is a finitely generated R-module without torsion. We now apply Lemma 9.7 □

Lemma 9.9. *Suppose that K is a field, R is a K-algebra and $a \in M^{\mathbb{N}}$ is a linear R-recurrence sequence of order d. Then there exists a ring R' which is finitely generated over K, a finitely generated R'-module M' and a R'-recurrence sequence $a' \in (M')^{\mathbb{N}}$ such that*

$$\mathcal{Z}(a) = \mathcal{Z}(a').$$

Proof. There exists a nonnegative integer m and $\alpha_0, \ldots, \alpha_{m-1} \in R$ such that

$$E^m a = \sum_{i=0}^{m-1} \alpha_i E^i a.$$

Set $R' := K[\alpha_0, \ldots, \alpha_{m-1}]$. Then a is also an linear R'-recurrence sequence. Let N be the R'-module generated by $a, Ea, E^2a, E^3a, \ldots$. Then N is finitely generated. In fact, it is generated by $a, Ea, E^2a, \ldots, E^{m-1}a$. Let M' be the module generated by $a(0), a(1), a(2), \ldots$. Then M' is a finitely generated R'-module because it is a homomorphic image of the finitely generated module N via the homomorphism $a \mapsto a(0)$. Take $a' = a$. □

Proof of Theorem 1.2. By Lemma 9.9 we may assume that R is finitely generated commutative $\mathbb{Q}$-algebra and M is finitely generated as an R-module. We apply Lemma 9.6. There exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_l \subseteq R$, R-modules $M_1, M_2, \ldots, M_l$ with M_i $\mathfrak{p}_i$-coprimary for all i, recurrence sequences $a_i \in M_i^{\mathbb{N}}$ for all i such that

$$\mathcal{Z}(a) = \bigcap_{i=1}^{l} \mathcal{Z}(a_i).$$

By Lemma 9.8, $\mathcal{Z}(a_i)$ is a union of a finite set and finitely many arithmetic progressions for all i. But then $\mathcal{Z}(a)$ also is a union of a finite set and finitely many arithmetic progressions. □

Lemma 9.10. *Suppose that A is an elementary p-nested set of order l which is up to a finite set contained in a p-nested set B of order d. Then $l \leq d$.*

Proof. This follows from

$$\delta_A(n) = \Omega(\log(n)^l)$$

and

$$\delta_B(n) = O(\log(n)^d).$$

□

Proof of Theorem 1.9. Suppose that K is an infinite field containing $\mathbb{F}_p$ (for example $K = \overline{\mathbb{F}}_p$, the algebraic closure). We may view a as a $R \otimes_{\mathbb{F}_p} K$-sequence in $M \otimes_{\mathbb{F}_p} K \supseteq M$ rather than in M. This shows that we may assume that R contains an infinite field without loss of generality.

By Lemma 9.9 we may assume that R is finitely generated K-algebra and M is finitely generated as an R-module. By Lemma 9.6 and Lemma 9.5, we can reduce to the case where there exists a prime ideal $\mathfrak{p} \subseteq R$ such that M is $\mathfrak{p}$-coprimary.

By Lemma 9.8, $\mathcal{Z}(a)$ is p-normal. However, it is not yet clear that $\mathcal{Z}(a)$ is p-normal *of order* $\leq d - 2$. We prove Theorem 1.9 by induction on t where t is the smallest nonnegative integer such that $\mathfrak{p}^t M = 0$. The case $t = 0$ is clear.

We can write

$$\mathcal{Z}(a) = \left(F_1 \cup \bigcup_{i=1}^{\alpha} A_i \cup \bigcup_{i=1}^{\beta} B_i \right) \setminus F_2,$$

where F_1, F_2 are finite, A_i is an infinite arithmetic progression for all i and B_i elementary p-nested for all i. We may assume that all the arithmetic progressions A_i have the same period, say n. Since the intersection of a set of the form $S_q(c_0; c_1, \ldots, c_l)$ with $m + n\mathbb{Z}$ is a union of elementary p-nested sets of order $\leq l$ (see the proof of Lemma 9.5, Case 2), we may assume that each B_j is contained in $m + n\mathbb{Z}$ for some $m \in \mathbb{Z}$. Hence we may assume that $B_j \cap A_i = \emptyset$ for all i, j.

Suppose that $B_j = S_q(c_0; c_1, \ldots, c_l)$. We would like to show that $l \leq d - 2$. Let us write $\mathfrak{p} = (f_1, \ldots, f_k)$. Define

$$a' \in ((\mathfrak{p}M)^k)^{\mathbb{N}} \cong ((\mathfrak{p}M)^{\mathbb{N}})^k$$

by

$$a' = (f_1 a, f_2 a, \ldots, f_k a).$$

Then a' is a R-recurrence sequence of order $\leq d$. By the induction hypothesis, $\mathcal{Z}(a')$ is p-normal of order $\leq d - 2$. We can write

$$\mathcal{Z}(a') = \left(\bigcup_{i=1}^{\alpha'} A'_i \cup B' \right) \setminus F',$$

where F' is finite, A'_i is an infinite arithmetic progression for all i and B' is a p-nested set of order $d - 2$.

If $B_j \cap A'_i$ is finite for all i, then B_j is up to a finite set contained in B'. We get $l \leq d - 2$ by Lemma 9.10.

Suppose that $B_j \cap A'_i$ is infinite for some i. We can write $A'_i = m' + n'\mathbb{N}$ for some $m', n' \in \mathbb{Z}$. Then there exists a p-power q' and $c'_0, \ldots, c'_l \in \mathbb{Q}$ such that

$$S_{q'}(c'_0; c'_1, \ldots, c'_l) \subseteq B_j \cap A'_i \subset \mathcal{Z}(a) \cap (m' + n'\mathbb{Z}).$$

Now we have

$$\mathcal{Z}(a) \cap (m' + n'\mathbb{Z}) = L^{n'}_{m'}\big(\mathcal{Z}\big(T^{n'}_{m'}a\big)\big).$$

Since $m' + n'i \in \mathcal{Z}(a')$ for $i \gg 0$, we get

$$\big(T^{n'}_{m'}a\big)(i) \in N := \{f \in M | \mathfrak{p}f = (0)\}$$

for $i \gg 0$. Note that N is a finitely generated torsion-free $R/\mathfrak{p}$-module, and $T^{n'}_{m'}a$ is an $R/\mathfrak{p}$-recurrence sequence of order $\le d$. By Lemma 9.7, $\mathcal{Z}(T^{n'}_{m'}a)$ is p-normal of order $\le d - 2$. We have

$$S_q(c'_0; c'_1, \dots, c'_l) \subseteq L^{n'}_{m'}\big(\mathcal{Z}\big(T^{n'}_{m'}a\big)\big) \subseteq \mathcal{Z}(a)$$

and $L^{n'}_{m'}(\mathcal{Z}(T^{n'}_{m'}a))$ is p-normal of order $\le d - 2$. Since $S_q(c'_0; c'_1, \dots, c'_l) \subseteq B_j$ and $B_j \cap A_k = \emptyset$ for all k, the intersection of $S_q(c'_0; c'_1, \dots, c'_l)$ and any infinite arithmetic progression in $\mathcal{Z}(a)$ is finite. In particular, the intersection of $S_q(c'_0; c'_1, \dots, c'_l)$ and any infinite arithmetic progression in $L^{n'}_{m'}(\mathcal{Z}(T^{n'}_{m'}a))$ is finite. It follows that $S_q(c'_0; c'_1 \dots, c'_l)$ is up to a finite set contained in a p-nested set of order $\le d - 2$, so $l \le d - 2$ by Lemma 9.10. □

10. Open problems

Uniform bounds. Suppose that K is a field of characteristic 0 and $a \in K^{\mathbb{N}}$ is a non-degenerate K-recurrence sequence of order d. W.M. Schmidt (see [26]) proved that $|\mathcal{Z}|$ is bounded above by $\exp(\exp(\exp(3d \log d)))$, regardless of the field K. More generally, Schmidt proved (see [27]) for an arbitrary K-recurrence sequence $a \in K^{\mathbb{N}}$ (possibly degenerate) recurrence sequence of order d, that $\mathcal{Z}(a)$ is the union of A elements and B arithmetic progressions, where $A + B \le \exp(\exp(\exp(20d)))$.

In view of the results in characteristic 0, we conjecture that there exists a constant $c(d)$, such that for every field K of characteristic $p > 0$, and every K-recurrence sequence $a \in K^{\mathbb{N}}$ order d, we can write

$$\mathcal{Z}(a) = X \setminus Y,$$

where X is the union of a A elements, B arithmetic progressions, C elementary nested sets of order $\le d - 2$ and Y is a finite set with at most D elements, such that $A + B + C + D \le c(d)$.

***S*-unit equations.** Suppose that K is a field and $\Gamma \subseteq K^\star$ is a finitely generated subgroup. Fix $\beta_1, \dots, \beta_d \in K$ and consider the set $\mathcal{F}_\Gamma(\beta_1, \dots, \beta_d)$ of all $(\alpha_1, \dots, \alpha_d) \in \Gamma^d$ such that

$$\beta_1\alpha_1 + \cdots + \beta_d\alpha_d = 1 \tag{24}$$

and no proper subsum

$$\beta_{i_1}\alpha_{i_1} + \cdots + \beta_{i_m}\alpha_{i_m}$$

with $1 \leq i_1 < i_2 < \cdots < i_m \leq d$ and $1 \leq m < d$ is equal to 0. If K has characteristic 0 then $\mathcal{F}_\Gamma(\beta_1, \ldots, \beta_d)$ is finite (see [22]). In that case an upper bound for the number of elements of $\mathcal{F}_\Gamma(\beta_1, \ldots, \beta_d)$ may be given in terms of the number of generators of Γ and d (see [7,5,6]).

If K has positive characteristic then $\mathcal{F}_\Gamma(\beta_1, \ldots, \beta_d)$ may be infinite. Solutions of (24) in positive characteristic were studied by Masser in [19]. His results are sufficient to solve a conjecture of Klaus Schmidt about mixing properties of algebraic $\mathbb{Z}^r$-actions. Our methods here may lead to a precise description of the solutions of (24) in positive characteristic.

In a recent preprint, Dragos Ghioca (see [10]) proved a version of the Mordell–Lang theorem in characteristic $p > 0$ (see also [1,11,20,21]). If we take (in the notation of [10]) $G = (\mathbb{G}_m)^d$, the d-dimensional torus, and $X \subset G$ the subvariety defined by

$$\beta_1 x_1 + \cdots + \beta_d x_d = 1,$$

then $\mathcal{F}_\Gamma(\beta_1, \ldots, \beta_d) = X(K) \cap \Gamma^d$ is described in the main theorem of that paper.

A nonlinear Skolem–Mahler–Lech theorem. A set of the form $m + n\mathbb{Z} \subseteq \mathbb{Z}$ with $m \in \mathbb{Z}$ and n a positive integer is called a doubly infinite arithmetic progression. The following theorem was recently proven by Jason Bell [2].

Theorem 10.1. *Suppose that Y is an affine variety over a field K of characteristic 0, $X \subseteq Y$ is a Zariski closed subset, $y \in Y$, and $\sigma : Y \to Y$ is an automorphism. The set*

$$\{n \in \mathbb{Z} | \sigma^n(y) \in X\}$$

is a union of a finite set and a finite number of doubly infinite arithmetic progressions.

Bell generalized the methods used in the proof of the Skolem–Mahler–Lech theorem (in characteristic 0) to prove this result. Given the results in this paper, it is natural to conjecture the following:

Conjecture 10.2. Suppose that Y is an affine variety over a field K of characteristic $p > 0$, X is a Zariski closed subset, $y \in Y$ and $\sigma : Y \to Y$ is an automorphism. Then the set

$$\{n \in \mathbb{Z} | \sigma^n(y) \in X\}$$

is a union of a finite set, finitely many doubly infinite arithmetic progressions and finitely many sets of the form

$$\widetilde{S}_q(c_0; c_1, c_2, \ldots, c_s).$$

References

1. Abramovich, D., Voloch, J.F.: Toward a proof of the Mordell–Lang conjecture in characteristic p. Int. Math. Res. Notices **5**, 103–115 (1992)
2. Bell, J.: A generalized Skolem–Mahler–Lech theorem for affine varieties. math.NT/0501309 (preprint)
3. Bézivin, J.-P.: Suites récurrentes linéaires en caractéristique non nulle. Bull. Soc. Math. France **115**, 227–239 (1987)
4. Eisenbud, D.: Commutative Algebra – with a View toward Algebraic Geometry. Springer, New York (1994)
5. Evertse, J.-H., Schlickewei, H.P.: The absolute subspace theorem and linear equations. In: Number Theory in Progress, vol. 1, pp. 121–142. de Gruyter, Berlin (1999)
6. Evertse, J.-H., Schlickewei, H.P.: A quantitative version of the absolute subspace Theorem. J. Reine Angew. Math. **548**, 21–127 (2002)
7. Evertse, J.-H., Schlickewei, H.P., Schmidt, W.: Linear equations in variables which lie in a multiplicative group. Ann. Math. **155**, 807–836 (2002)
8. Furstenberg, H.: Recurrence in Ergodic Theory and Combinatorial Number Theory. Princeton University Press, Princeton, NJ (1981)
9. Everest, G., van der Poorten, A., Shparlinski, I., Ward, T.: Recurrence Sequences, Mathematical Surveys and Monographs, vol. 104. Am. Math. Soc., Providence, RI (2003)
10. Ghioca, D.: The isotrivial case in the Mordell–Lang Theorem. Preprint, to appear in Trans. Am. Math. Soc.
11. Hrsushovski, E.: The Mordell–Lang conjecture for function fields. J. Am. Math. Soc **9**(3), 667–690 (1996)
12. Kitchens, B., Schmidt, K.: Mixing sets and relative entropies for higher-dimensional Markov shifts. Ergodic Theory Dyn. Syst. **13**(4), 705–735 (1993)
13. Lang, S.: Algebra. Graduate Texts in Mathematics, vol. 211, revised 3rd ed. Springer, New York (2002)
14. Lech, C.: A note on recurring series. Ark. Mat. **2**, 417–421 (1953)
15. Lewis, H., Papadimitriou, C.: Elements of the Theory of Computation. Prentice-Hall (1981)
16. Mahler, K.: Eine arithmetische Eigenschaft der Taylor Koeffizienten rationaler Funktionen. Proc. Akad. Wet. Amsterdam **38**, 51–60 (1935)
17. Mahler, K.: On the Taylor coefficients of rational functions. Proc. Cambridge Philos. Soc. **52**, 39–48 (1956), Addendum: **53**, 544 (1957)
18. Masser, D.: Two letters to D. Behrend. September 12 and 19, 1985
19. Masser, D.: Mixing and linear equations over groups in positive characteristic. Israel J. Math. **142**, 189–204 (2004)
20. Moosa, R., Scanlon, T.: F-structures and integral points on semi-abelian varieties over finite fields. Am. J. Math. **126**, 473–522 (2004)
21. Moosa, R., Scanlon, T.: The Modell–Lang conjecture in positive characteristic revisited. In: Model, Theory and Applications. Quad. Mat., vol. 11, pp. 273–296. Aracne, Rome (2002)
22. van der Poorten, A.: Additive relations in number fields. Séminaire de théorie des nombres de Paris 1982–1983. Progress in Mathematics, pp. 259–266. Birkhäuser, Bosten, MA (1984)
23. Schlickewei, H.P., Schmidt, W.: The number of solutions of polynomial-exponential equations. Compos. Math. **120**(2), 193–225 (2000)
24. Schmidt, K.: Dynamical systems of Algebraic Origin. Prog. Math., vol. 128. Birkhäuser, Basel (1995)
25. Schmidt, W.: Heights of points on subvarieties of $\mathbb{G}_m^n$. In: Number Theory (Paris, 1993–1994). London Math. Soc. Lecture Note Ser., vol. 235, pp. 157–187. Cambridge Univ. Press, Cambridge (1996)
26. Schmidt, W.: The zero multiplicity of linear recurrence sequences. Acta Math. **182**, 243–282 (1999)

27. Schmidt, W.: Zeros of linear recurrence sequences. Publ. Math. **56**, 609–630 (2000)
28. Skolem, T.: Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen. In: Comptes rendus du congrés des mathèmaticiens scandinaves, Stockholm, 1934, pp. 163–188. (1935)
29. Stepanov, S., Shparlinski, I.: On the construction of a primitive normal basis of a finite field (Russian), Mat. Sb. **180**(8), 1067–1972, 1151 (1989). Translation in Math. USSR-Sb. **67**(2), 527–533 (1990)
30. Stepanov, S., Shparlinski, I.: On the construction of primitive elements and primitive normal bases in a finite field. In: Computational Number Theory (Debrecen, 1989), pp. 1–14. de Gruyter, Berlin (1991)
31. Szemerédi, E.: On sets of integers containing no *k* elements in arithmetic progression. Acta Arith. **27**, 199–245 (1975)