Available online at www.sciencedirect.com

ScienceDirect

Indagationes Mathematicae 26 (2015) 113–136

indagationes mathematicae

www.elsevier.com/locate/indag

Linear equations over multiplicative groups, recurrences, and mixing II

H. Derksen[a,*], D. Masser[b]

[a] *Department of Mathematics, University of Michigan, East Hall 530 Church Street, Ann Arbor, MI 48109, USA*
[b] *Mathematisches Institut, Universität Basel, Rheinsprung 21, 4051 Basel, Switzerland*

Received 16 December 2013; received in revised form 1 August 2014; accepted 10 August 2014

Communicated by F. Beukers

Abstract

Let $u_1, \ldots, u_m$ be linear recurrences with values in a field K of positive characteristic p. We show that the set of integer vectors $(k_1, \ldots, k_m)$ such that $u_1(k_1) + \cdots + u_m(k_m) = 0$ is p-normal in a natural sense generalizing that of the first author, who proved the result for $m = 1$. Furthermore the set is effectively computable if K is. We illustrate this with an example for $m = 4$. We also show that the corresponding set for zero characteristic is not decidable for $m = 557844$, thus verifying a conjecture of Cerlienco, Mignotte, and Piras.

Keywords: Recurrence sequences; Skolem–Mahler–Lech theorem; Algebraical dynamical systems; Mixing

1. Introduction

In 2004 the second author published a paper [20] about linear equations over multiplicative groups in positive characteristic. This was specifically aimed at an application to a problem about mixing for dynamical systems of algebraic origin, and as a result about linear equations it lacked some of the simplicity of the classical results in zero characteristic. A new feature was the appearance of $n - 1$ independently operating Frobenius maps; here n is the number of variables.

* Corresponding author. Tel.: +1 734 763 2309.
E-mail addresses: hderksen@umich.edu (H. Derksen), David.Masser@unibas.ch (D. Masser).

http://dx.doi.org/10.1016/j.indag.2014.08.002

In 2007 the first author published a paper [7] about recurrences in positive characteristic. He proved an analogue of the famous Skolem–Lech–Mahler Theorem in zero characteristic. A new feature was the appearance of integer sequences involving combinations of $d-2$ powers of the characteristic; here d is the order of the recurrence.

It turns out that these two new features are identical. In positive characteristic the vanishing of a recurrence with d terms can be regarded as a linear equation in $d-1$ variables to be solved in a multiplicative group (so in particular $n-1=d-2$). This observation can be developed in three directions.

In Part I of this series [8] we gave an improved version of the result of [20] in a form more closely related to that in zero characteristic. Here in Part II we show how to recover the result of [7], and in fact we shall generalize it to sums of recurrences. In zero characteristic there are rather few results on such sums, and indeed there is a conjecture of Cerlienco, Mignotte, and Piras [6] to the effect that such problems are undecidable (see later). In positive characteristic we will establish not only the decidability but also give completely effective algorithms to solve the problem. In Part III of the series [9] we present some new applications to mixing problems for dynamical systems of algebraic origin. We apply the linear equations result to give an effective algorithm for determining the smallest order of non-mixing of any basic action associated with a given prime ideal in a Laurent polynomial ring. We also show how to determine effectively all non-mixing sets of that order.

Recall that a map u from $\mathbf{N}_0=\{0,1,2,\ldots\}$ to a field K is called a recurrence sequence if there exist d in $\mathbf{N}=\{1,2,\ldots\}$ and $\lambda_1,\ldots,\lambda_d$ in K such that

$$u(k+d)=\lambda_1 u(k+d-1)+\cdots+\lambda_d u(k) \tag{1.1}$$

for all k in $\mathbf{N}_0$. For example the Fibonacci sequence

$$u(0)=0,\qquad u(1)=1,\qquad u(k+2)=u(k+1)+u(k)\quad (k=0,1,2,\ldots)$$

with $d=2$, which proceeds

$$0,1,1,2,3,5,8,13,21,34,55,89,\mathbf{144},233,377,610,\ldots,$$

where we have highlighted the largest perfect power $u(12)=144=12^2$ [5] in the sequence. In fact if we change this to π to get a "Pibonacci" sequence

$$0,1,1,2,3,5,8,13,21,34,55,89,\pi,233,377,610,\ldots,$$

then it remains a recurrence sequence, though now with $d=15$ and $u(k+15)=u(k+14)+u(k+13)$ $(k=0,1,2,\ldots)$. In particular $\lambda_d=0$.

Or the Berstel sequence defined by

$$u(0)=u(1)=0,\qquad u(2)=1,$$
$$u(k+3)=2u(k+2)-4u(k+1)+4u(k)\quad (k=0,1,2,\ldots)$$

which starts

$$0,0,1,2,0,-4,0,16,16,-32,-64,64,256,0,-768,$$

and then after a gap of 36 terms continues

$$-884763262976,0,2731599200256,\ldots.$$

The more recent literature also considers maps u from $\mathbf{Z}$ to K satisfying (1.1) for all k in $\mathbf{Z}$. Then it is no restriction to assume $\lambda_d \neq 0$. For example the Fibonacci sequence can be infinitely extended backwards in a unique way (as in [25] p. 171); but the changed sequence cannot be infinitely extended backwards at all.

We begin by recalling some results in zero characteristic. An infinite arithmetic progression is a set of the form $a, a+b, a+2b, \ldots$, with $a \geq 0$ in $\mathbf{Z}$ and b in $\mathbf{N}$. We could include singletons by allowing $b = 0$, but we do not. The following is the Skolem–Lech–Mahler Theorem.

Theorem A. *Let K_0 be a field of zero characteristic, and let u be a recurrence sequence from $\mathbf{N}_0$ to K_0. Then the set of k in $\mathbf{N}_0$ with $u(k) = 0$ is a union of finitely many singletons and infinite arithmetic progressions.*

Several authors have studied more elaborate equations involving recurrences. For example, Evertse [11] considered solutions k, h of $u(k) = u(h)$, and similarly Laurent [15] the equation

$$u(k) = v(h) \tag{1.2}$$

where v is a second recurrence. In [16] he also studied $u(k) = Au(h)$ (note that constant multiples of recurrence sequences are again recurrence sequences). His Théorème 2 (p.26) there explicitly mentions the possibility of subgroups of $\mathbf{Z}^2$ showing up in the solution set. This, generalized to $\mathbf{Z}^m$, will be a key feature of our present work in positive characteristic. Then Schlickewei and Schmidt [21] treated (1.2) when $u = Aw^r$ and $v = Bw^s$ for fixed constants A, B, fixed positive integers r, s and a fixed recurrence w (note also that powers of recurrence sequences are again recurrence sequences). They mention the possibility of one-parameter linear families, which again amount to subgroups of $\mathbf{Z}^2$. And finally Schlickewei and Schmidt [22] considered solutions k, h, l of

$$Au(k) + Bu(h) + Cu(l) = 0 \tag{1.3}$$

for fixed constants A, B, C. They also found that the solution set of (1.2) can be described with linear or exponential families of a single integral parameter κ, and the same for (1.3) as long as K_0 is the field of all algebraic numbers. There seem to be no similar results for sums of four or more recurrences. But they conjectured that an analogous description is possible, even for quite general equations

$$u_1(k_1) + \cdots + u_m(k_m) = 0. \tag{1.4}$$

However Losert [19] has given the counterexample

$$2^k + h.2^h - l.2^l = 0$$

with a doubly exponential family of solutions

$$(k, h, l) = (\kappa + 2.2^\kappa + 2^\kappa.2^{2^\kappa},\ 2^\kappa.2^{2^\kappa},\ 2^\kappa + 2^\kappa.2^{2^\kappa}).$$

A less elegant type of counterexample is

$$2^k + (\sqrt{2}.2^h - h) + (\sqrt{3}.2^l - \sqrt{2}.l) - \sqrt{3}.j = 0$$

which can be written as

$$(2^k - h) + \sqrt{2}.(2^h - l) + \sqrt{3}.(2^l - j) = 0 \tag{1.5}$$

so leading to triply exponential solutions

$$(k, h, l, j) = (\kappa, 2^{\kappa}, 2^{2^{\kappa}}, 2^{2^{2^{\kappa}}})$$

(compare [22] p. 227).

Now to positive characteristic. Here Theorem A is false in characteristic p; for example the map

$$u(k) = (t+1)^k - t^k - 1$$

is a recurrence sequence for the function field $K = \mathbf{F}_p(t)$ because

$$u(k+3) = (2t+2)u(k+2) - (t^2+3t+1)u(k+1) + (t^2+t)u(k).$$

However $u(k) = 0$ for all $k = p^f$ $(f = 0, 1, 2, \ldots)$, and it is easy to see (for example directly by differentiation or by using the general techniques of [7] Section 3) that there are no other k with this property.

The correct versions in positive characteristic were found by the first author in [7]. As well as singletons and infinite arithmetic progressions we need the notion of an elementary nested set. However it is convenient first to do things over $\mathbf{Z}$. This necessitates the notion of a doubly infinite arithmetic progression $a + b\mathbf{Z}$; and we can again restrict to b in $\mathbf{N}$.

Fix a prime p and a positive integer e, and put $q = p^e$. For a positive integer g and rational $c_0, c_1, \ldots, c_g$ with $(q-1)c_0, (q-1)c_1, \ldots, (q-1)c_g$ in $\mathbf{Z}$ and $c_0 + c_1 + \cdots + c_g$ in $\mathbf{Z}$ we define $D_q(c_0; c_1, \ldots, c_g)$ as the set of all $c_0 + c_1 q^{f_1} + \cdots + c_g q^{f_g}$ $(f_1, \ldots, f_g = 0, 1, 2, \ldots)$. The conditions on $c_0, c_1, \ldots, c_g$ easily imply (see [7] p. 177) that $D_q(c_0; c_1, \ldots, c_g)$ lies in $\mathbf{Z}$. We call it an elementary p-nested set in $\mathbf{Z}$ of order at most g (maybe it can be defined with fewer summands). Then we define a p-normal set in $\mathbf{Z}$ of order at most g as a finite union of singletons, doubly infinite arithmetic progressions and elementary p-nested sets in $\mathbf{Z}$ of order at most g. We can interpret this for $g = 0$ in the obvious way by omitting the p-nested sets.

Finally we say that the recurrence satisfying (1.1) has order at most d. Now we can state the first version in positive characteristic.

Theorem B1. *Let K be a field of positive characteristic p, and let u be a recurrence sequence from $\mathbf{Z}$ to K of order at most $d \geq 2$. Then the set of k in $\mathbf{Z}$ with $u(k) = 0$ is p-normal in $\mathbf{Z}$ of order at most $d - 2$.*

In fact this assertion does not appear explicitly in [7], which is apparently restricted to maps u from $\mathbf{N}_0$. But it can easily be deduced from the results in [7]. It is also the special case $m = 1$ of our Theorem 1 below (whose proof is essentially independent of that of [7]).

For the version over $\mathbf{N}_0$, denote by $S_q(c_0; c_1, \ldots, c_g)$ (when $g \geq 1$) the intersection $D_q(c_0; c_1, \ldots, c_g) \cap \mathbf{N}_0$. It is easy to see that this intersection is infinite if and only if at least one of $c_1, \ldots, c_g$ is positive. In this case we call $S_q(c_0; c_1, \ldots, c_g)$ an elementary p-nested set in $\mathbf{N}_0$ of order at most g. We consider a union of a finite number of singletons in $\mathbf{N}_0$, infinite arithmetic progressions in $\mathbf{N}_0$, and elementary p-nested sets in $\mathbf{N}_0$ of order at most g, and we further allow the removal of finitely many singletons (another feature special to positive characteristic); what remains will be called p-normal in $\mathbf{N}_0$ of order at most g. Again we can interpret this for $g = 0$ in the obvious way. Thus the p-normal sets in $\mathbf{N}_0$ are precisely what we get by intersecting $\mathbf{N}_0$ with p-normal sets in $\mathbf{Z}$ and then removing a finite number of singletons.

Theorem B2. *Let K be a field of positive characteristic p, and let u be a recurrence sequence from $\mathbf{N}_0$ to K of order at most $d \geq 2$. Then the set of k in $\mathbf{N}_0$ with $u(k) = 0$ is p-normal in $\mathbf{N}_0$ of order at most $d - 2$.*

This is the same as Theorem 1.8 of [7] (p. 178).

In both these theorems the bounds $d - 2$ are best possible. This follows indirectly from the observation in [8] (p. 1079) that the corresponding bound $n - 1$ there is best possible. But here we give a simple direct proof.

The main result of the present paper generalizes Theorems B1 and B2 to arbitrary sums of recurrences $u_1, \ldots, u_m$ and solutions of (1.4). Here the new feature involves additive subgroups, which makes it now especially convenient to do things first over $\mathbf{Z}^m$.

Take p, e, q, g as above, at first with $g \geq 1$. For $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_g$ in $\mathbf{Q}^m$ with $(q-1)\mathbf{c}_0$, $(q-1)\mathbf{c}_1, \ldots, (q-1)\mathbf{c}_g$ in $\mathbf{Z}^m$ and $\mathbf{c}_0 + \mathbf{c}_1 + \cdots + \mathbf{c}_g$ in $\mathbf{Z}^m$ we define $D_q(\mathbf{c}_0; \mathbf{c}_1, \ldots, \mathbf{c}_g)$ as the set of all $\mathbf{c}_0 + \mathbf{c}_1 q^{f_1} + \cdots + \mathbf{c}_g q^{f_g}$ $(f_1, \ldots, f_g = 0, 1, 2, \ldots)$. The conditions on $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_g$ easily imply that $D_q(\mathbf{c}_0; \mathbf{c}_1, \ldots, \mathbf{c}_g)$ lies in $\mathbf{Z}^m$. We call it an elementary p-nested set in $\mathbf{Z}^m$ of order at most g. Finally we define a p-normal set in $\mathbf{Z}^m$ of order at most g as a finite union of singletons and sums $H + D$, where H is a subgroup of $\mathbf{Z}^m$ and D is either a singleton or an elementary p-nested set in $\mathbf{Z}^m$ of order at most g. Again we can allow also $g = 0$. It is easy to see that this agrees with the earlier definition when $m = 1$, because if H is non-zero then it has the form $b\mathbf{Z}$ with b in $\mathbf{N}$, and now $H + D$ is simply the finite union of all doubly infinite arithmetic progressions $a + b\mathbf{Z}$ with $0 \leq a < b$ which meet D.

Theorem 1. *Let K be a field of positive characteristic p, and let $u_1, \ldots, u_m$ be recurrence sequences from $\mathbf{Z}$ to K of respective orders at most $d_1, \ldots, d_m$ with $d_1 + \cdots + d_m \geq 2$. Then the set of $\mathbf{k} = (k_1, \ldots, k_m)$ in $\mathbf{Z}^m$ with*

$$u_1(k_1) + \cdots + u_m(k_m) = 0$$

is p-normal in $\mathbf{Z}^m$ of order at most $d_1 + \cdots + d_m - 2$.

There is no essential difficulty in deducing a version over $\mathbf{N}_0^m$. But it seems to be not especially elegant; for example it is not quite sufficient merely to intersect everything with $\mathbf{N}_0^m$ and remove some singletons. Just for completeness we present such a version, postponing the somewhat inelegant definition of p-normal in $\mathbf{N}_0^m$ to Section 5.

Theorem 2. *Let K be a field of positive characteristic p, and let $u_1, \ldots, u_m$ be recurrence sequences from $\mathbf{N}_0$ to K of respective orders at most $d_1, \ldots, d_m$ with $d_1 + \cdots + d_m \geq 2$. Then the set of $\mathbf{k} = (k_1, \ldots, k_m)$ in $\mathbf{N}_0^m$ with*

$$u_1(k_1) + \cdots + u_m(k_m) = 0$$

is p-normal in $\mathbf{N}_0^m$ of order at most $d_1 + \cdots + d_m - 2$.

We should say something about effectivity.

In zero characteristic Theorem A remains ineffective, even for rational recurrences of order 5 like

$$u(k) = (8+i)^k + (8-i)^k - (7+4i)^k - (7-4i)^k - 1, \tag{1.6}$$

(for which we thank Maurice Mignotte), where we still cannot in principle find all the k with $u(k) = 0$ (the trouble is $|8+i| = |8-i| = |7+4i| = |7-4i|$). But there are many estimates

for the number of solutions. For example, Beukers [4] showed that if a rational recurrence of order at most 3 has only finitely many zeros, then it has at most 6, as in the Berstel sequence. The more recent estimates from [12] imply the upper bound $\exp(2.18^9) = \exp(396718580736)$ for the number of k in (1.6). Very recently Amoroso and Viada [2] have improved the results of [12], giving $24^{1620} < \exp(5149)$. And more generally Schmidt [26] showed in Theorem A for order at most d that at most $\exp\exp\exp(20d)$ singletons and infinite arithmetic progressions are needed. The works [21,22] cited above, as well as [23] and [24], also contain explicit estimates for the number of solutions.

In fact Cerlienco, Mignotte and Piras in [6] (p. 104) have conjectured that for some m the existence of a solution of (1.4) in zero characteristic is undecidable in the logical sense. It seems to us that this is true, but in a somewhat trivial fashion when $u_1, \dots, u_m$ are just polynomials. In fact we prove here that $m = 557844$ suffices for undecidability over the field of all algebraic numbers. By contrast our remarks below imply that in positive characteristic this problem is always decidable (provided the underlying field K is).

In positive characteristic the first author had already noted in [7] that his method, expressed in the language of automata, yielded fully effective results for Theorems B1 and B2. For example Corollary 6.7 (p. 203) gives an explicit upper bound for all k with

$$u(k) = b_1 a_1^k + \cdots + b_d a_d^k = 0$$

when there are only finitely many; here $b_1, a_1, \dots, b_d, a_d$ are arbitrary polynomials in $\mathbf{F}_q[t]$.

Our own proofs, based on [8], are equally effective. Thus in Theorem 1 we see a finite union of $H + D$, and we could give estimates for generators of the subgroups H as well as for the q and $\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_g$ in the nested sets $D = D_q(\mathbf{c}_0; \mathbf{c}_1, \dots, \mathbf{c}_g)$. These estimates would involve certain heights of quantities like those generalizing $b_1, a_1, \dots, b_d, a_d$ above. In particular since $H + D_q(\mathbf{c}_0; \mathbf{c}_1, \dots, \mathbf{c}_g)$ contains $\mathbf{c}_0 + \mathbf{c}_1 + \cdots + \mathbf{c}_g$ they would deliver an explicit search bound for a single solution of (1.4) which would show that the analogue of the Cerlienco–Mignotte–Piras Conjecture in positive characteristic is false. However we give no such estimates in the present paper.

Instead we determine the complete set of solutions of (1.4) for several examples $u_1, \dots, u_m$. Thus we solve $u(k) + v(h) = 0$ in $\mathbf{Z}^2$ with

$$u(k) = ks((-1)^k - 1^k), \qquad v(h) = (h+1)\left((t+1)^h - t^h - 1^h\right) \tag{1.7}$$

in $\mathbf{F}_p(s,t)$ for $p \geq 3$ and independent variables s, t. Here we are able to argue directly without the machinery of [8]. And following (1.2) and (1.3) for sums of two and three recurrences we also treat a sum of four recurrences. This involves

$$u(k) = t^k + (1-t)^k \tag{1.8}$$

which could be regarded as an analogue of the Fibonacci sequence.

Theorem 3. *The set of (k, h, l, j) in $\mathbf{N}_0^4$ with*

$$u(k) + u(h) + u(l) + u(j) = 0 \tag{1.9}$$

for (1.8) in $\mathbf{F}_2[t]$ is the union of seventeen sets $\mathbf{N}_0^4 \cap (H + D)$, where H is a subgroup of $\mathbf{Z}^4$ and D is elementary 2-nested in $\mathbf{Z}^4$ of order at most four.

This can be interpreted as the determination of all non-mixing sets of a particular shape of cardinality eight for the Ledrappier example [17] (see also the paper [3] of Arenas-Carmona,

Berend and Bergelson). For the proof we also argue directly, but this time using the basic method in [8], that of differentiating with respect to t, together with an inductive argument. Leitner has also used differentiation in [18], where he deals with equations that involve four terms; however (1.9) implicitly involves eight terms and the approach in [18] might become too tedious, especially in low characteristics like 2.

Here is how this paper is arranged. In Section 2 we prove a preliminary result about nested sets in arbitrary finitely generated abelian groups. We apply this in Section 3 to deduce Theorem 1, and then we give some simple examples including (1.7) in Section 4.

In Section 5 we prove Theorem 2 after defining p-normal sets in $\mathbf{N}_0^m$, and in Section 6 we prove Theorem 3 in a more precise form.

Then in Appendix A we give a simple direct proof that the bound $d-2$ in Theorems B1 and B2 (and so also in Theorems 1 and 2) is best possible. And in Appendix B we prove that the Conjecture of Cerlienco, Mignotte and Piras is true, even for a sum of 557844 recurrences.

After writing the first draft of this paper, we became aware of the work [1] of Adamczewski and Bell. In their Theorem 2.1 (p. 350) they show that the set in our Theorem 2 is p-automatic in a natural sense generalizing that of [7], and furthermore that it can be effectively determined. However not all p-automatic sets are p-normal. We thank Boris Adamczewski for showing us [1].

2. Nested sets in abelian groups

Let $\mathcal{C}$ be a finitely generated abelian group. For q a power of a prime p, $g \geq 1$ and C_0, $C_1, \ldots, C_g$ in $\mathcal{C}$ we define $U_q(C_0; C_1, \ldots, C_g)$ as the set of all

$$C_0 + C_1 q^{f_1} + \cdots + C_g q^{f_g} \quad (f_1 \geq 0, \ldots, f_g \geq 0) \tag{2.1}$$

in $\mathcal{C}$. This can be extended to $g = 0$ to signify the singleton $\{C_0\}$. It looks like a nested set; however the coefficients $C_0, C_1, \ldots, C_g$ have no denominators. We call it an elementary integral p-nested set of order at most g.

The main result needed to deduce our Theorems 1 and 2 from [8] is the following.

Proposition 2.1. *Let $B_1, \ldots, B_m$ be in $\mathcal{C}$, let $\mathcal{B}$ be a subgroup of $\mathcal{C}$, and denote by H the subgroup of all $(k_1, \ldots, k_m)$ in $\mathbf{Z}^m$ such that $k_1 B_1 + \cdots + k_m B_m$ lies in $\mathcal{B}$. Let U be an elementary integral p-nested set of order at most g in $\mathcal{C}$. Then the set of all $(k_1, \ldots, k_m)$ in $\mathbf{Z}^m$ such that $k_1 B_1 + \cdots + k_m B_m$ lies in $\mathcal{B} + U$ is either empty or $H + \mathcal{D}$, where $\mathcal{D}$ is a finite union of singletons and elementary p-nested sets of order at most g in $\mathbf{Z}^m$.*

We need some preliminary remarks.

Lemma 2.1. *Suppose $c_0 q^{f_0} + c_1 q^{f_1} + \cdots + c_g q^{f_g} = 0$ for integers $c_0, c_1, \ldots, c_g$ not all zero. Then there are i, j with $0 \leq i \neq j \leq g$ such that $1 \leq q^{f_i - f_j} \leq |c_0| + |c_1| + \cdots + |c_g|$.*

Proof. This is essentially part of the proof of Lemma 9.3 of [7] (p. 214), which is used there for a similar purpose. We can suppose that $f_0 \leq f_1 \leq \cdots \leq f_g$ and also $c_g \neq 0$. Now

$$q^{f_g} \leq |c_g q^{f_g}| = |c_0 q^{f_0} + c_1 q^{f_1} + \cdots + c_{g-1} q^{f_{g-1}}| \leq (|c_0| + |c_1| + \cdots + |c_{g-1}|) q^{f_{g-1}}.$$

So here we can take $i = g$, $j = g - 1$.

Lemma 2.2. *Let $\mathcal{A}$ be a subgroup of $\mathcal{C}$. Then there is a finite set Φ of ϕ in either* $\mathrm{Hom}(\mathcal{C}, \mathbf{Z})$ *or* $\mathrm{Hom}(\mathcal{C}, \mathbf{Z}/r\mathbf{Z})$ *for prime powers r such that $\mathcal{A}$ is the set of A in $\mathcal{C}$ with $\phi(A) = 0$ for every ϕ in Φ.*

Proof. By the structure theorem on abelian groups the quotient $\mathcal{C}/A$ is isomorphic to a product of copies of $\mathbf{Z}$ and $\mathbf{Z}/r\mathbf{Z}$ for prime powers r, and so we can take ϕ as the corresponding projections.

Lemma 2.3. *Let $\mathcal{A}$ be a subgroup of $\mathcal{C}$ defined as above by a finite set Φ of ϕ in either* $\mathrm{Hom}(\mathcal{C}, \mathbf{Z})$ *or* $\mathrm{Hom}(\mathcal{C}, \mathbf{Z}/r\mathbf{Z})$. *Let U be an elementary integral p-nested set of order at most g in $\mathcal{C}$ defined by (2.1), and suppose that not all $\phi(C_i)$ $(i = 0, 1, \ldots, g)$ are zero for some ϕ in Φ in* $\mathrm{Hom}(\mathcal{C}, \mathbf{Z})$. *Then either $\mathcal{A} \cap U$ is empty or there is a finite union $\mathcal{U}'$ of elementary integral p-nested sets of order at most $g - 1$ inside U such that $\mathcal{A} \cap U = \mathcal{A} \cap \mathcal{U}'$.*

Proof. If $\mathcal{A} \cap U$ is non-empty let $A = C_0 + C_1 q^{f_1} + \cdots + C_g q^{f_g}$ be an arbitrary element of $\mathcal{A} \cap U$. Then $c_0 + c_1 q^{f_1} + \cdots + c_g q^{f_g} = 0$ for some ϕ in Φ and $c_i = \phi(C_i)$ $(i = 0, \ldots, g)$ in $\mathbf{Z}$ with at least one of $c_0, c_1, \ldots, c_g$ non-zero. By Lemma 2.1 (with $f_0 = 0$) there are distinct i, j with $0 \le f_i - f_j \le L$ for some L independent of A. Suppose that $f_i - f_j = l$ for some l with $0 \le l \le L$, with for example $i < j$. Now $C_i q^{f_i} + C_j q^{f_j} = (q^l C_i + C_j) q^{f_j}$, and if $i \ne 0$ this means that A lies in the elementary integral p-nested set

$$U(i, j, l) = U_q(C_0; C_1, \ldots, C_{i-1}, C_{i+1}, \ldots, C_{j-1}, q^l C_i + C_j, C_{j+1}, \ldots, C_g)$$

of order at most $g - 1$ in $\mathcal{C}$. It is just as easy to see that $U(i, j, l)$ lies in U. If $i = 0$ we use $U_q(C_0 + q^l C_j; C_1, \ldots, C_{j-1}, C_{j+1}, \ldots, C_g)$. Similar arguments work if $i > j$. Thus if we define the finite union $\mathcal{U}' = \bigcup_{i \ne j} \bigcup_{l=0}^{L} U(i, j, l)$ then we see that $\mathcal{A} \cap U$ lies in $\mathcal{A} \cap \mathcal{U}'$; and since $\mathcal{U}'$ lies in U we deduce equality here. This completes the proof.

Lemma 2.4. *Let $\mathcal{A}$ be a subgroup of $\mathcal{C}$. Let s be a positive integer prime to p, and let ϕ be in* $\mathrm{Hom}(\mathcal{C}, \mathbf{Z}/s\mathbf{Z})$ *with $\phi = 0$ on $\mathcal{A}$. Let U be an elementary integral p-nested set of order at most g in $\mathcal{C}$ defined by (2.1). Then there is a finite union $\mathcal{U}$ of elementary integral p-nested sets inside U of order at most g on which $\phi = 0$ such that $\mathcal{A} \cap U = \mathcal{A} \cap \mathcal{U}$.*

Proof. Let w be the multiplicative order of q modulo s. For an element $C_0 + C_1 q^{f_1} + \cdots + C_g q^{f_g}$ of U as in (2.1) we can write $f_i = \tilde{f}_i w + d_i$ $(i = 1, \ldots, g)$ with $\tilde{f}_i \ge 0$ and $0 \le d_i < w$. Accordingly U splits into a disjoint union of $\tilde{U} = U_{\tilde{q}}(C_0; \tilde{C}_1, \ldots, \tilde{C}_g)$ with $\tilde{q} = q^w \equiv 1 \pmod{s}$ and $\tilde{C}_i = q^{d_i} C_i$ $(i = 1, \ldots, g)$. Thus ϕ takes on $\tilde{U}$ the constant value $\phi(\tilde{U}) = \phi(C_0) + \phi(\tilde{C}_1) + \cdots + \phi(\tilde{C}_g)$; and in intersecting with $\mathcal{A}$ we can restrict to those $\tilde{U}$ with $\phi(\tilde{U}) = 0$. This completes the proof.

Lemma 2.5. *Let $\mathcal{A}$ be a subgroup of $\mathcal{C}$. Let r be a positive integer which is a power of p, and let ϕ be in* $\mathrm{Hom}(\mathcal{C}, \mathbf{Z}/r\mathbf{Z})$ *with $\phi = 0$ on $\mathcal{A}$. Let U be an elementary integral p-nested set of order at most g in $\mathcal{C}$ defined by (2.1). Then if $\phi(C_0) \ne 0$ there is a finite union $\mathcal{U}'$ of elementary integral p-nested sets inside U of order at most $g - 1$ with $\mathcal{A} \cap U = \mathcal{A} \cap \mathcal{U}'$; while if $\phi(C_0) = 0$ there is a finite union $\mathcal{U}'$ of elementary integral p-nested sets inside U of order at most $g - 1$ and an elementary integral p-nested set $\tilde{U}$ inside U of order at most g on which $\phi = 0$ such that $\mathcal{A} \cap U = (\mathcal{A} \cap \mathcal{U}') \cup (\mathcal{A} \cap \tilde{U})$.*

Proof. For an element $C_0 + C_1 q^{f_1} + \cdots + C_g q^{f_g}$ in $\mathcal{A} \cap U$ we have $c_0 + c_1 q^{f_1} + \cdots + c_g q^{f_g} = 0$ with $c_i = \phi(C_i)$ $(i = 0, \ldots, g)$. If $c_0 \ne 0$ in $\mathbf{Z}/r\mathbf{Z}$ then this forces some $ef_i < d$, where $q = p^e$

and $r = p^d$. So in this case we can reduce to $\mathcal{U}'$ of lower order by replacing C_0 by $C_0 + C_i q^{f_i}$ much as in the proof of Lemma 2.3.

If $c_0 = 0$ then we have just $c_1 q^{f_1} + \cdots + c_g q^{f_g} = 0$. Now we can split off the elements with $ef_i < d$, if any, into $\mathcal{U}'$ as above. Those with $ef_i \geq d$ make up a elementary integral p-nested set $\tilde{U}$ of order at most g, because this says $f_i \geq l$ for some fixed l and we can replace C_i by $C_i q^l$. It is clear that $\phi = 0$ on $\tilde{U}$. This completes the proof.

Proof of Proposition 2.1. We start with the special case $\mathcal{B} = 0$. So we are looking for the set $\mathbf{K}$ of all $\mathbf{k} = (k_1, \ldots, k_m)$ in $\mathbf{Z}^m$ with $k_1 B_1 + \cdots + k_m B_m$ in U, with U defined say by (2.1). We use induction on g.

Suppose $g = 0$. We have to solve $k_1 B_1 + \cdots + k_m B_m = C_0$. But this is clearly a coset of H, so $H + \mathcal{U}$ for a singleton $\mathcal{U}$.

Next assume that it is done for $g - 1$ powers of q ($g \geq 1$), still with $\mathcal{B} = 0$. We are going to use Lemmas 2.2–2.5 above with $\mathcal{A} = \mathbf{Z}B_1 + \cdots + \mathbf{Z}B_m$ to reduce to the situation when U already lies in $\mathcal{A}$.

We use Lemma 2.2 for $\mathcal{A}$ to obtain Φ. If the conditions of Lemma 2.3 are satisfied, then either $\mathcal{A} \cap U$ is empty or there is a finite union $\mathcal{U}'$ of elementary integral p-nested sets of order at most $g - 1$ in $\mathcal{C}$ such that $\mathcal{A} \cap U = \mathcal{A} \cap \mathcal{U}'$. In the first case $\mathbf{K}$ is empty, so we are done. In the second case our condition on $\mathbf{k}$ says that $k_1 B_1 + \cdots + k_m B_m$ lies in one of the elementary integral p-nested sets of order at most $g - 1$ in $\mathcal{U}'$, and so the desired conclusion follows by induction.

If the conditions of Lemma 2.3 are not satisfied, then $\phi(C_i) = 0$ for all i and all ϕ in Φ in $\mathrm{Hom}(\mathcal{C}, \mathbf{Z})$. We want to deduce a similar assertion for the other ϕ in $\mathrm{Hom}(\mathcal{C}, \mathbf{Z}/r\mathbf{Z})$.

Assume first that $r = s$ is prime to p. For a ϕ in Φ in $\mathrm{Hom}(\mathcal{C}, \mathbf{Z}/s\mathbf{Z})$ we use Lemma 2.4 to see that $\mathcal{A} \cap U$ is a finite union of $\mathcal{A} \cap \tilde{U}$ for $\tilde{U}$ in U of order at most g with $\phi = 0$ on $\tilde{U}$. For a second such $\tilde{\phi}$ we similarly reduce each $\tilde{U}$ to finitely many $\tilde{\tilde{U}}$ in $\tilde{U}$ with $\tilde{\phi} = 0$ on $\tilde{\tilde{U}}$. And so on. We conclude that $\mathcal{A} \cap U$ is a finite union of $\mathcal{A} \cap U_0$ with $\phi = 0$ on U_0 for all ϕ in Φ in $\mathrm{Hom}(\mathcal{C}, \mathbf{Z}/s\mathbf{Z})$.

The upshot is that we can reduce to the case where all the ϕ in Φ in $\mathrm{Hom}(\mathcal{C}, \mathbf{Z}/s\mathbf{Z})$ (s prime to p) vanish on the new U_0. Still all the ϕ in Φ in $\mathrm{Hom}(\mathcal{C}, \mathbf{Z})$ vanish on the new U_0, because the new U_0 is a subset of the original U.

Otherwise if r is a power of p then for a ϕ in Φ in $\mathrm{Hom}(\mathcal{C}, \mathbf{Z}/r\mathbf{Z})$ we use Lemma 2.5. If $\phi(C_0) \neq 0$ we can lower the order and use the induction hypothesis. If $\phi(C_0) = 0$ we can either do this or reduce to the case when ϕ vanishes on U. Repeating this with the other ϕ, we see that we can assume that all the ϕ in Φ in $\mathrm{Hom}(\mathcal{C}, \mathbf{Z}/r\mathbf{Z})$ vanish on the new U. As above the other ϕ in Φ in $\mathrm{Hom}(\mathcal{C}, \mathbf{Z}/s\mathbf{Z})$ and in $\mathrm{Hom}(\mathcal{C}, \mathbf{Z})$ vanish on the new U. But this means that we have indeed reduced the Proposition to the situation when U already lies in $\mathcal{A}$!

This means that every element (2.1) lies in $\mathcal{A}$. In particular

$$C_0 + C_1 + \cdots + C_g = n_1 B_1 + \cdots + n_m B_m \tag{2.2}$$

for $\mathbf{n} = (n_1, \ldots, n_m)$ in $\mathbf{Z}^m$. Also $C_0 + C_1 + \cdots + C_g q$ is in $\mathcal{A}$. Subtracting shows that $(q-1)C_g$ is in $\mathcal{A}$. Similarly considering $C_0 + C_1 + \cdots + C_{g-1} q + C_g q$ shows that $(q-1)C_{g-1}$ is in $\mathcal{A}$. And so on until $(q-1)C_1$; but also by (2.2) $(q-1)C_0$ too. So we get equations

$$(q-1)C_i = n_{i1} B_1 + \cdots + n_{im} B_m \quad (i = 0, \ldots, g) \tag{2.3}$$

for $\mathbf{n}_i = (n_{i1}, \ldots, n_{im})$ $(i = 0, \ldots, g)$ in $\mathbf{Z}^m$. Putting these back into (2.2) gives $l_1 B_1 + \cdots + l_m B_m = 0$ for $\mathbf{l} = (l_1, \ldots, l_m) = \mathbf{n}_0 + \mathbf{n}_1 + \cdots + \mathbf{n}_g - (q-1)\mathbf{n}$. Thus by definition $\mathbf{l}$ lies in H

(still $\mathcal{B} = 0$). We now define

$$\mathbf{c}_i = \frac{1}{q-1}\mathbf{n}_i \quad (i = 1, \dots, g), \qquad \mathbf{c}_0 = \frac{1}{q-1}(\mathbf{n}_0 - \mathbf{l})$$

so that $(q-1)\mathbf{c}_i$ lies in $\mathbf{Z}^m$ $(i = 0, \dots, g)$ and $\mathbf{c}_0 + \cdots + \mathbf{c}_g = \mathbf{n}$ lies in $\mathbf{Z}^m$ too. So the set of $\mathbf{c}_0 + \mathbf{c}_1 q^{f_1} + \cdots + \mathbf{c}_g q^{f_g}$ is an elementary p-nested set D_0 in $\mathbf{Z}^m$ of order at most g. We now show that $\mathbf{K}$ is none other than $H + D_0$.

Well, some $\mathbf{k} = (k_1, \dots, k_m)$ is in $\mathbf{K}$ if and only if $k_1 B_1 + \cdots + k_m B_m = C_0 + \sum_{i=1}^{g} C_i q^{f_i}$; and the right-hand side is by (2.2) and (2.3)

$$\sum_{j=1}^{m} n_j B_j + \sum_{i=1}^{g} C_i (q^{f_i} - 1) = \sum_{j=1}^{m} n_j B_j + \sum_{i=1}^{g} \left(\frac{q^{f_i} - 1}{q-1} \right) \sum_{j=1}^{m} n_{ij} B_j.$$

So the condition on $\mathbf{k}$ is equivalent to

$$\mathbf{k} \equiv \mathbf{n} + \sum_{i=1}^{g} \left(\frac{q^{f_i} - 1}{q-1} \right) \mathbf{n}_i \equiv \mathbf{n} + \sum_{i=1}^{g} \mathbf{c}_i (q^{f_i} - 1) \equiv \mathbf{c}_0 + \sum_{i=1}^{g} \mathbf{c}_i q^{f_i} \bmod H;$$

that is, just $\mathbf{k}$ in $H + D_0$ as claimed. This settles the special case $\mathcal{B} = 0$ of the Proposition.

Now for the general case. We can write $\mathcal{B} = \mathbf{Z}A_1 + \cdots + \mathbf{Z}A_n$. By the special case just done, the set of $(k_1, \dots, k_m, j_1, \dots, j_n)$ in $\mathbf{Z}^{m+n}$ with $k_1 B_1 + \cdots + k_m B_m + j_1 A_1 + \cdots + j_n A_n$ in U is either empty or $\tilde{H} + \tilde{\mathcal{D}}$, where $\tilde{\mathcal{D}}$ is a finite union of singletons and elementary p-nested sets of order at most g in $\mathbf{Z}^{m+n}$. Here $\tilde{H}$ is just the set of $(k_1, \dots, k_m, j_1, \dots, j_n)$ with $k_1 B_1 + \cdots + k_m B_m + j_1 A_1 + \cdots + j_n A_n = 0$. We are interested in the projection ρ of this to $\mathbf{Z}^m$ corresponding to the first m factors. Now $\rho(\tilde{H} + \tilde{\mathcal{D}}) = \rho(\tilde{H}) + \rho(\tilde{\mathcal{D}})$, and the first summand is the set of $(k_1, \dots, k_m)$ with $k_1 B_1 + \cdots + k_m B_m$ in $\mathcal{B}$; this is exactly what we need in the Proposition. Finally it is obvious that the projection of an elementary p-nested set of order at most g in $\mathbf{Z}^{m+n}$ is an elementary p-nested set of order at most g in $\mathbf{Z}^m$. This completes the proof of the Proposition.

3. Proof of Theorem 1

As mentioned, we can assume $\lambda_d \neq 0$ in (1.1). Then we have the familiar representation

$$u(k) = \sum_{i=1}^{r} \sum_{l=0}^{e_i - 1} \beta_i^{(l)} \binom{k}{l} \alpha_i^k \tag{3.1}$$

for any recurrence u from $\mathbf{N}_0$ to K of order at most d; here the $\beta_i^{(l)}, \alpha_i$ are in the algebraic closure of K, the $\binom{k}{l}$ are binomial coefficients, and $\sum_{i=1}^{r} e_i \leq d$. One can consult [10] (p. 4) with $\mathbf{N}$ instead of $\mathbf{N}_0$, or [6] (pp. 70, 71) with $n_0 = -1$. In these two references the binomial coefficients appear in two different forms $\binom{k+a}{b}$ $(b = 0, \dots, e-1)$ but it is well-known that these are all integer linear combinations of the above $\binom{k}{l}$ $(l = 0, \dots, e-1)$. Further we have $\alpha_i \neq 0$ $(i = 1, \dots, r)$ as they are the zeroes of the characteristic polynomial ([10] p. 1) whose constant term is $-\lambda_d$. Thus the right-hand side of (3.1) makes sense for $k < 0$, and continues to satisfy the relation (1.1). It follows from the remarks in Section 1 that (3.1) holds on all of $\mathbf{Z}$.

Now there is a power Q of p such that all the $\binom{k}{l}$ in (3.1) depend only on the values of k modulo Q. This enables us to take each $e_i = 1$ (related to the notion of simplicity in

Definition 2.3 of [7] p. 182). Thus for all k in each fixed residue class $k_0 + Q\mathbf{Z}$ in $\mathbf{Z}$ we may write (3.1) as $u(k) = \sum_{i=1}^{d} \beta_i \alpha_i^k$ (this step is of course impossible in zero characteristic).

In proving Theorem 1 we can assume that each recurrence has this form. This is because for any $\mathbf{k}_0$ in $\mathbf{Z}^m$ and $H + D$ in Theorem 1 the set $\mathbf{k}_0 + Q(H + D) = \tilde{H} + \tilde{D}$ for the subgroup $\tilde{H} = QH$ and the elementary p-nested set $\tilde{D} = \mathbf{k}_0 + QD$.

Our basic Eq. (1.4) therefore becomes

$$\sum_{j=1}^{m} \sum_{i=1}^{d_j} \beta_{ij} \alpha_{ij}^{k_j} = 0. \tag{3.2}$$

We are going to apply [8] to the linear variety V defined by the corresponding equation

$$\sum_{j=1}^{m} \sum_{i=1}^{d_j} \beta_{ij} X_{ij} = 0. \tag{3.3}$$

Thus we are in projective $\mathbf{P}_n$ with $n = d_1 + \cdots + d_m - 1$. We work inside the field generated by the β_{ij}, α_{ij} over $\mathbf{F}_p$, and G as the radical (inside this field) of the group generated by the α_{ij}. This G is also finitely generated (see for example [20] p. 195). Now (3.2) gives a point π on $V(G)$. It has a diagonal form resulting from the special exponents. In fact we may identify the group G^n with $\mathbf{P}_n(G)$ and define an isomorphism log from these to a finitely generated additive abelian group $\mathcal{C}$. Then

$$\log \pi = k_1 B_1 + \cdots + k_m B_m, \tag{3.4}$$

where B_j is the log of the point with $X_{ij} = \alpha_{ij}$ $(i = 1, \ldots, d_j)$ and $X_{rs} = 1$ elsewhere.

Now Theorem 2 (p. 1049) of [8] shows that $V(G)$ is a finite union of sets $T = (\pi_0, \pi_1, \ldots, \pi_d)_q S(G)$ with points $\pi_0, \pi_1, \ldots, \pi_d$ $(0 \le d \le n - 1)$ defined over G and linear subgroups S defined by equations $X_{ij} = X_{rs}$. Here

$$(\pi_0, \pi_1, \ldots, \pi_d)_q = \pi_0 \bigcup_{f_1=0}^{\infty} \cdots \bigcup_{f_d=0}^{\infty} (\varphi^{f_1} \pi_1) \cdots (\varphi^{f_d} \pi_d),$$

with φ the Frobenius corresponding to the power q of p and of course the interpretation π_0 itself if $d = 0$. A point π_T in T has

$$\log \pi_T = C_0 + C_1 q^{f_1} + \cdots + C_d q^{f_d} + B \tag{3.5}$$

with $C_h = \log \pi_h$ $(h = 0, 1, \ldots, d)$ and $B = \log \sigma$ for some σ in $S(G)$. Thus the set of all such $\log \pi_T$ forms a sum $\mathcal{B} + U$, where U is an elementary integral p-nested set of order at most

$$d \le n - 1 = d_1 + \cdots + d_m - 2 \tag{3.6}$$

in $\mathcal{C}$ as in (2.1), and $\mathcal{B} = \log S(G)$. This latter is a subgroup of $\mathcal{C}$ because $S(G)$ is a group. Comparing (3.4) and (3.5), we see that for each T the set of $\mathbf{k} = (k_1, \ldots, k_m)$ arising is exactly as in our Proposition, a sum $H_T + \mathcal{D}_T$. Here H_T is the group of all $\mathbf{k}$ with $k_1 B_1 + \cdots + k_m B_m$ in $\mathcal{B}$ and $\mathcal{D}_T$ is a finite union of singletons and elementary p-nested sets in $\mathbf{Z}^m$, which by (3.6) are of order at most $d_1 + \cdots + d_m - 2$.

And now we see that Theorem 1 has dropped out.

4. Some examples

The p-normal set in Theorem 1 involves a finite union of sums $H + D$. In an earlier version of this result we had just a single subgroup H. The following simple example shows that this must have been wrong. Write $u(k) = t^k + (\frac{1}{t})^k$ and take $m = 2$ with the second recurrence $v(h) = -u(h)$ in $K = \mathbf{F}_p(t)$. It is easy to see that the zero-sum set of (k, h) in $\mathbf{Z}^2$ with $u(k) + v(h) = 0$ is the union of the subgroups $\mathbf{Z}(1, 1)$ and $\mathbf{Z}(1, -1)$.

We also worked out the following more elaborate example illustrating the same mistake.

Consider the two recurrences

$$u(k) = ks((-1)^k - 1^k), \qquad v(h) = (h + 1)\left((t + 1)^h - t^h - 1^h\right) \tag{4.1}$$

in $K = \mathbf{F}_p(s, t)$ for $p \geq 3$ and independent variables s, t. Now the solutions depend on k and h modulo p. There are seven cases.

(1) $k \not\equiv 0, h \equiv 0$. Now $u(k) + v(h) = 0$ if and only if $u(k) = v(h) = 0$, thanks to the factor s. Without the factors $k, h + 1$ in (4.1) we get the Cartesian product $2\mathbf{Z} \times Q$ in $\mathbf{Z} \times \mathbf{Z} = \mathbf{Z}^2$, where $Q = \{p^e;\ e = 0, 1, 2, \ldots\}$. This is the group sum $H + D$ of H with an elementary p-nested set $D = (0, 1)Q$ in $\mathbf{Z}^2$, where $H = 2\mathbf{Z} \times \{0\}$ in $\mathbf{Z}^2$. Taking account of the factors $k, h + 1$ and the congruences we see that k is restricted to one of the arithmetic progressions $k_0 + 2p\mathbf{Z}$ ($0 \leq k_0 < 2p,\ k_0$ even) and h to $e \geq 1$. We find $H_1 + D_1$ with

$$H_1 = 2p\mathbf{Z} \times \{0\}, \qquad D_1 = \{(k_0, 0) + (0, p)p^f;\ f = 0, 1, 2, \ldots\}.$$

(2) $k \equiv 0, h \equiv 0$. Now we find $H_2 + D_2$ with

$$H_2 = p\mathbf{Z} \times \{0\}, \qquad D_2 = \{(0, p)p^f;\ f = 0, 1, 2, \ldots\}.$$

(3) $k \not\equiv 0, h \equiv 1$. Again at first we get $H + D$ above, and the congruences give $k_0 + 2p\mathbf{Z}$ and this time $e = 0$ in Q. We find $H_3 + D_3$ with

$$H_3 = 2p\mathbf{Z} \times \{0\}, \qquad D_3 = \{(k_0, 1)\},$$

so that D_3 is now a singleton.

(4) $k \equiv 0, h \equiv 1$. We find $H_4 + D_4$ with

$$H_4 = p\mathbf{Z} \times \{0\}, \qquad D_4 = \{(0, 1)\}.$$

(5) $k \not\equiv 0, h \equiv -1$. We find $H_5 + D_5$ with

$$H_5 = 2p\mathbf{Z} \times p\mathbf{Z}, \qquad D_5 = \{(k_0, -1)\},$$

so that H_5 now has full rank 2.

(6) $k \equiv 0, h \equiv -1$. We find $H_6 + D_6$ with

$$H_6 = p\mathbf{Z} \times p\mathbf{Z}, \qquad D_6 = \{(0, -1)\}.$$

(7) $h \not\equiv 0, 1, -1$. Now $h = p^e$; but this is 0 or 1 modulo p, so there are no solutions here.

Thus we see four different groups H_1, H_2, H_5, H_6. Maybe their number can be reduced by noting that some are of finite index in others. They all happen to be Cartesian products $G_1 \times G_2$ but this is due to the splitting effect of the variable s in (4.1). The simple example

$$u(k) = t^k, \qquad v(h) = -t^h$$

also in $K = \mathbf{F}_p(t)$ has the zero-sum set $H = \mathbf{Z}(1, 1)$ which is not a Cartesian product.

For the version over $\mathbf{N}_0^m$ we already remarked that it is not quite sufficient merely to intersect everything with $\mathbf{N}_0^m$ and remove some singletons, as is the case $m = 1$ in Theorem B2. Consider the case $m = 2$ and the example

$$u(k) = t^k + (1-t)^k, \qquad v(h) = -t^h - (1-t)^h$$

now in characteristic two with $K = \mathbf{F}_2(t)$. It can be seen without too much trouble, for example by exploiting the term $k(-t)^{k-1}$ in $u(k)$, or simply by referring to Lemma 6.2 below, that the zero-sum set of (k, h) in $\mathbf{Z}^2$ with $u(k) + v(h) = 0$ is the union of $H = \mathbf{Z}(1, 1)$ and the points

$$(2^e, 2^f) = (1, 0)2^e + (0, 1)2^f \quad (e, f = 0, 1, 2, \ldots);$$

the latter make up an elementary 2-nested set of order 2. This can also be deduced from the work [18] of Leitner. If we change $v(12)$, as in the Fibonacci sequence, to Carlitz's analogue π_2 of π which is transcendental over K (see for example [13] pp. 51, 52), then clearly the effect is indeed to remove the single point (12, 12). But if it is instead $v(1)$ that we change to π_2, then we lose all the points

$$(2^e, 1) = (0, 1) + (1, 0)2^e \quad (e = 0, 1, 2, \ldots);$$

which make up an elementary 2-nested set of order 1.

5. Proof of Theorem 2

In fact the last example above illustrates the arguments of this proof. Generally to solve $u(k) + v(h) = 0$ on $\mathbf{N}_0^2$ we first change u, v on finite sets F, E so that they can be extended backwards to $\mathbf{Z}$. Off the finite set $F \times E$ usually k is not in F and h is not in E, and we get in $\mathbf{Z}^2$ a p-normal set S then to be intersected with the set $\mathbf{N}_0''$ of (k, h) in $\mathbf{N}_0^2$ with k not in F and h not in E. Or h might be in E and then the set $S(h)$ of k is p-normal in $\mathbf{Z}$ (as now $v(h)$ is a constant recurrence). Thus we get a union of $S(h) \times h$, and we must now intersect with $\mathbf{N}_0' \times h$, where $\mathbf{N}_0'$ is $\mathbf{N}_0$ with F removed. Similarly if k is in F.

This leads us inexorably to the definition of p-normal in $\mathbf{N}_0^m$. To begin with it involves a finite Cartesian product $\mathcal{F} = F_1 \times \cdots \times F_m$, with $F_1, \ldots, F_m$ finite in $\mathbf{Z}$. This gives rise to a disjoint union

$$\mathbf{Z}^m = \bigcup_I \mathbf{Z}_{\mathcal{F}}(I) \tag{5.1}$$

taken over all subsets I of $\{1, \ldots, m\}$, where $\mathbf{Z}_{\mathcal{F}}(I)$ is defined by requiring that k_i lies in F_i for i in I and k_i does not lie in F_i for i not in I. For example the biggest $\mathbf{Z}_{\mathcal{F}}(I)$ comes from the empty set I, when it is $\mathbf{Z}^m$ minus some coordinate hyperplanes. When I is a singleton, $\mathbf{Z}_{\mathcal{F}}(I)$ consists of some of these hyperplanes minus lower-dimensional coordinate spaces, and so on, down to $\mathbf{Z}_{\mathcal{F}}(I) = \mathcal{F}$ for the full set $I = \{1, \ldots, m\}$.

When I is not empty, each of the $\mathbf{Z}_{\mathcal{F}}(I)$ in turn splits into a disjoint union

$$\mathbf{Z}_{\mathcal{F}}(I) = \bigcup_{f \in F(I)} \mathbf{Z}_{\mathcal{F}}(I, f) \tag{5.2}$$

where $F(I)$ is the product of the F_i for i in I. However we take the ordering of Cartesian products seriously or rather pedantically here and choose for each I a permutation $\sigma = \sigma_I$ with $\sigma(\{m - l + 1, \ldots, m\}) = I$, where $l = |I|$, so that $F(I) = F_{\sigma(m-l+1)} \times \cdots \times F_{\sigma(m)}$. Then $\mathbf{Z}_{\mathcal{F}}(I, f)$ is the subset of $\mathbf{Z}_{\mathcal{F}}(I)$ defined by $(k_{\sigma(m-l+1)}, \ldots, k_{\sigma(m)}) = f$.

This $\mathbf{Z}_{\mathcal{F}}(I, f)$ lies in the set $\overline{\mathbf{Z}_{\mathcal{F}}(I, f)}$ defined by ignoring the requirements for i not in I. Using also σ for the same permutation on coordinates, we have

$$\mathbf{Z}_{\mathcal{F}}(I, f) \subseteq \overline{\mathbf{Z}_{\mathcal{F}}(I, f)} = \sigma(\mathbf{Z}^{m-l} \times f). \tag{5.3}$$

For empty I we can interpret (5.2) and (5.3) just by dropping f and taking σ as the identity.

For example if $m = 1$ and $\mathcal{F} = F_1 = F$ (say) then $\mathbf{Z}_{\mathcal{F}}(I) = F$ for $I = \{1\}$ and $\mathbf{Z}_{\mathcal{F}}(I, f) = \{f\}$ for each f in F; and $\mathbf{Z}_{\mathcal{F}}(I)$ for empty I is the complement of F in $\mathbf{Z}$.

Next we have to repeat the whole thing over $\mathbf{N}_0$. If now $\mathcal{F}$ lies in $\mathbf{N}_0^m$, then we get a disjoint union

$$\mathbf{N}_0^m = \bigcup_I \bigcup_{f \in F(I)} \mathbf{N}_{\mathcal{F}}(I, f) \tag{5.4}$$

simply by intersecting (5.1) and (5.2) with $\mathbf{N}_0^m$. And of course still

$$\mathbf{N}_{\mathcal{F}}(I, f) \subseteq \sigma(\mathbf{Z}^{m-l} \times f)$$

as in (5.3).

Finally we say that a subset S of $\mathbf{N}_0^m$ is p-normal in $\mathbf{N}_0^m$ of order at most g if there is a finite Cartesian product $\mathcal{F}$ as above and for each I and f in $F(I)$ a p-normal set $S(I, f)$ in $\mathbf{Z}^{m-l}$ of order at most g such that

$$S = \bigcup_I \bigcup_{f \in F(I)} (\mathbf{N}_{\mathcal{F}}(I, f) \cap \sigma(S(I, f) \times f)) \tag{5.5}$$

with f and σ omitted when I is empty.

For example if $m = 1$ and $\mathcal{F} = F_1 = F$ (say) then $I = \{1\}$ in (5.5) contributes the finite set $F \cap \mathbf{N}_0$ and the empty I contributes $S_0 \cap \mathbf{N}_0$ with any points from F removed, where S_0 is p-normal in $\mathbf{Z}$. Thus the resulting S is indeed p-normal in $\mathbf{N}_0$ in the sense of [7].

We can now prove Theorem 2. Given recurrences $u_1, \ldots, u_m$ on $\mathbf{N}_0$, we can change u_i on a finite set F_i to get a recurrence u_i^* on $\mathbf{Z}$. For by Lemma 2.4 of [7] (p.183) the recurrence u_i from some point onwards is basic. This means $\lambda_d \neq 0$ in (1.1) and so infinite extension backwards is possible. Put $\mathcal{F} = F_1 \times \cdots \times F_m$ in $\mathbf{N}_0^m$. For each I and each f in $F(I)$ we get a f_i in F_i for i in I. Consider the equation $(\sum_{i \notin I} u_i^*(k_i)) + u = 0$ or more pedantically

$$u_{\sigma(1)}^*(k_{\sigma(1)}) + \cdots + u_{\sigma(m-l)}^*(k_{\sigma(m-l)}) + u = 0 \tag{5.6}$$

with $u = \sum_{i \in I} u_i(f_i)$. Regarding u as a constant recurrence of order at most 1, we see from Theorem 1 that the solution set $S(I, f)$ in $\mathbf{Z}^{m-l}$ of (5.6) is a p-normal set in $\mathbf{Z}^{m-l}$ of order at most

$$\left(\sum_{i \notin I} d_i\right) + 1 - 2 \leq d_1 + \cdots + d_m - 2, \tag{5.7}$$

at least if I is non-empty; however if I is empty then there is no u in (5.6) and so no 1 in (5.7). Now we see that the zero-sum set of (1.4) in $\mathbf{N}_0^m$ intersected with $\mathbf{N}_{\mathcal{F}}(I, f)$ is

$$\mathbf{N}_{\mathcal{F}}(I, f) \cap \sigma(S(I, f) \times f). \tag{5.8}$$

This is because on $\mathbf{N}_{\mathcal{F}}(I, f)$ we know that k_i is not in F_i for i not in I (so $i = \sigma(j)$ for some j as in (5.6)) and $u_i(k_i) = u_i^*(k_i)$ here, and $k_i = f_i$ for i in I so $\sum_{i \in I} u_i(k_i) = \sum_{i \in I} u_i(f_i) = u$

here; thus we get precisely (5.6). Now Theorem 2 follows from (5.5) by taking the union in (5.8) and remembering (5.4).

6. Proof of Theorem 3

In fact we will prove the following explicit version.

Theorem 3′. *Up to permutations of the non-negative integers k, h, l, j, the set of solutions of (1.9) is the union of the following five sets*

$$\{(k, k, l, l);\ k, l = 0, 1, 2, \ldots\}, \tag{6.1}$$

$$\{(k, k, 2^\lambda, 2^\theta);\ k, \lambda, \theta = 0, 1, 2, \ldots\}, \tag{6.2}$$

$$\{(2^\kappa, 2^\eta, 2^\lambda, 2^\theta);\ \kappa, \eta, \lambda, \theta = 0, 1, 2, \ldots\}, \tag{6.3}$$

$$\{(2^\alpha + 2^\beta, 2^\beta + 2^\gamma, 2^\gamma + 2^\alpha, 2^\theta);\ \alpha, \beta, \gamma, \theta = 0, 1, 2, \ldots\}, \tag{6.4}$$

$$\{(2^\alpha + 2^\gamma, 2^\beta + 2^\gamma, 2^\alpha + 2^\delta, 2^\beta + 2^\delta);\ \alpha, \beta, \gamma, \delta = 0, 1, 2, \ldots\}. \tag{6.5}$$

To see the connexion with Theorem 3, we proceed to verify that each of the above sets has the form $\mathbf{N}_0^4 \cap (H + D)$.

For (6.1) the H is defined by $k = h, l = j$; and $D = 0$.

For (6.2) the H is defined by $k = h, l = j = 0$; and $D = D_2(\mathbf{0}; \mathbf{e}_l, \mathbf{e}_j)$, where

$$\mathbf{e}_l = (0, 0, 1, 0), \qquad \mathbf{e}_j = (0, 0, 0, 1)$$

are standard unit vectors.

For the remaining sets $H = 0$ and the sets D are respectively

$$D_2(\mathbf{0}; \mathbf{e}_k, \mathbf{e}_h, \mathbf{e}_l, \mathbf{e}_j)$$

$$D_2(\mathbf{0}; \mathbf{e}_k + \mathbf{e}_h, \mathbf{e}_h + \mathbf{e}_l, \mathbf{e}_l + \mathbf{e}_k, \mathbf{e}_j)$$

$$D_2(\mathbf{0}; \mathbf{e}_k + \mathbf{e}_l, \mathbf{e}_h + \mathbf{e}_j, \mathbf{e}_k + \mathbf{e}_h, \mathbf{e}_l + \mathbf{e}_j)$$

with

$$\mathbf{e}_k = (1, 0, 0, 0), \qquad \mathbf{e}_h = (0, 1, 0, 0).$$

After permutations the sets in Theorem 3′ give rise to respectively to 3, 6, 1, 4, 3 similar sets, giving 17 in all. This proves Theorem 3.

For a positive integer k write $\omega(k)$ for the number of ones in the binary expansion of k, with $\omega(0) = 0$.

Lemma 6.1. *The polynomial $u(k) = t^k + (1-t)^k$ in $\mathbf{F}_2[t]$ is the sum of $2^{\omega(k)} - 1$ distinct powers of t.*

Proof. If k is the sum of distinct powers $k_1, \ldots, k_r$ of 2 then $r = \omega(k)$ and

$$(1-t)^k = (1-t)^{k_1 + \cdots + k_r} = (1-t)^{k_1} \cdots (1-t)^{k_r} = (1 - t^{k_1}) \cdots (1 - t^{k_r})$$

involves 2^r distinct powers of t, one of which is $t^{k_1 + \cdots + k_r} = t^k$. The result follows.

Lemma 6.2. *The set S_2 of (k, h) in $\mathbf{N}_0^2$ such that*

$$u(k) + u(h) = 0$$

is the union of

$$\{(k, k);\ k = 0, 1, 2, \ldots\}, \tag{6.2.1}$$

$$\{(2^\kappa, 2^\lambda);\ \kappa, \lambda = 0, 1, 2, \ldots\}. \tag{6.2.2}$$

Proof. This will set the pattern for the subsequent proofs. We write $S_2^?$ for the union of (6.2.1), (6.2.2). As $u(2^\kappa) = 1$ it is clear that $S_2^?$ lies in S_2. We prove the opposite inclusion by showing by induction on N that any (k, h) in S_2 with size $\max\{k, h\} = N$ lies in $S_2^?$. This is trivial for $N = 0$.

Thus assume that it holds for all sizes less than some $N \geq 1$. For a given (k, h) of size N we consider the various parities of the coordinates.

If h, k are both even then we can take square roots to get $u(\frac{1}{2}k) + u(\frac{1}{2}h) = 0$. So $\frac{1}{2}(k, h)$ is in S_2, with size $\frac{1}{2}N < N$. Therefore by induction it is in $S_2^?$. And so clearly (k, h) is also in $S_2^?$.

In the remaining cases we will need to differentiate, noting that

$$\frac{d}{dt}u(k) = ku(k - 1).$$

If k is even and h is odd then differentiating gives $u(h - 1) = 0$. This implies $h = 1$. But then $u(k) = 1$ which by Lemma 6.1 implies $2^{\omega(k)} - 1 = 1$ so $\omega(k) = 1$ so $k = 2^\kappa$. Thus (k, h) is in (6.2.2) and so $S_2^?$. A similar argument works for odd k and even h.

Finally suppose k, h are both odd. Then differentiation gives $u(k - 1) + u(h - 1) = 0$ so $(k - 1, h - 1)$ is in S_2 with size $N - 1 < N$. Therefore by induction it is in $S_2^?$. If in (6.2.1) then so is (k, h) and we are done. Else it is in (6.2.2), and then $k = 2^\kappa + 1,\ h = 2^\eta + 1$; but now we calculate

$$0 = u(k) + u(h) = t^{2^\kappa} + t^{2^\eta}.$$

This forces $\kappa = \eta,\ k = h$ and so (k, h) is in (6.2.1) so $S_2^?$. That completes the proof.

Lemma 6.3. *Up to permutations on k, h, the set S_{2t} of (k, h, l) in $\mathbf{N}_0^3$ such that*

$$u(k) + u(h) + t^l = 0$$

is

$$\{(2^\kappa, 0, 0);\ \kappa = 0, 1, 2, \ldots\}. \tag{6.3.1}$$

Proof. We follow the strategy of the previous proof, with $S_{2t}^?$ in (6.3.1) clearly contained in S_{2t}, and then inductively with (k, h, l) of size $\max\{k, h, l\} = N$.

If h, k, l are all even then we deduce that $\frac{1}{2}(k, h, l)$ is in S_{2t}; and then by induction in $S_{2t}^?$ so S_{2t}.

If k, h are even and l odd then differentiation gives at once a contradiction.

If h, l are even and k is odd then differentiating gives $u(k - 1) = 0$ so $k = 1$. But then

$$0 = u(k) + u(h) + t^l = 1 + u(h) + t^l$$

which by Lemma 6.1 implies $2^{\omega(h)} - 1 = 0$ or 2, so $\omega(h) = 0$ so $h = 0$ and $l = 0$ and we are in $S_{2t}^?$. A similar argument works for even k, l and odd h, and these cover all cases when two of k, h, l are even.

If k is even and h, l are odd then differentiation gives $u(h-1)+t^{l-1} = 0$. Now $2^{\omega(h-1)}-1 = 1$ so $h - 1 = 2^\eta$ and then $l = 1$. But now

$$0 = u(k) + u(h) + t^l = u(k) + 1 + t^{2^\eta}$$

impossible by Lemma 6.1. Similarly if h is even and k, l are odd.

If l is even and k, h are odd then differentiation gives $u(k-1)+u(h-1) = 0$ so $(k-1, h-1)$ is in the set S_2 of Lemma 6.2. If $k - 1 = h - 1$ then $0 = u(k) + u(h) + t^l = t^l$ impossible. So $k = 2^\kappa + 1,\ h = 2^\eta + 1$. But now

$$0 = u(k) + u(h) + t^l = t^{2^\kappa} + t^{2^\eta} + t^l$$

again impossible.

Finally suppose k, h, l are all odd. Then differentiation shows that $(k - 1, h - 1, l - 1)$ is in S_{2t}. So by induction in $S_{2t}^?$, and we can assume $k = 2^\kappa + 1,\ h = l = 1$. But then

$$0 = u(k) + u(h) + t^l = t^{2^\kappa}$$

another contradiction. This completes the proof.

Lemma 6.4. *Up to permutations, the set S_3 of (k, h, l) in $\mathbf{N}_0^3$ such that*

$$u(k) + u(h) + u(l) = 0$$

is the union of

$$\{(k, k, 0);\ k = 0, 1, 2, \ldots\}, \tag{6.4.1}$$

$$\{(2^\kappa, 2^\eta, 0);\ \kappa, \eta = 0, 1, 2, \ldots\}. \tag{6.4.2}$$

Proof. Again induction and parities, with $S_3^?$ in S_3 defined by (6.4.1) and (6.4.2).

If k, h, l are all even then we proceed via $\frac{1}{2}(k, h, l)$ as above.

If k, l are even and h is odd then differentiation gives $h = 1$. Now

$$0 = u(k) + u(h) + u(l) = u(k) + u(l) + 1$$

and so $(k, l, 0)$ lies in the set S_{2t} of Lemma 6.3. We deduce $k = 2^\kappa,\ l = 0$. Now (k, h, l) lies in (6.4.2). Similar arguments work if exactly two of k, h, l are even.

If l is even and k, h are odd then differentiation shows that $(k - 1, h - 1)$ lies in S_2 from Lemma 6.2. The case $k - 1 = h - 1$ leads to $l = 0$ and so (6.4.1). The other case $k - 1 = 2^\kappa,\ h - 1 = 2^\eta$ leads to

$$0 = u(k) + u(h) + u(l) = t^{2^\kappa} + t^{2^\eta} + u(l).$$

So by Lemma 6.1 we have $2^{\omega(l)} - 1 = 0$ or 2, so $l = 0,\ k = h$ and again we are in (6.4.1). Similar arguments work if exactly one of k, h, l is even.

Finally if k, h, l are all odd then we get $(k - 1, h - 1, l - 1)$ in S_3 so by induction in (6.4.1) or (6.4.2). The first leads to $k = h,\ l = 1$ clearly impossible. The second leads to $k = 2^\kappa + 1,\ h = 2^\eta + 1,\ l = 1$ and so

$$0 = u(k) + u(h) + u(l) = t^{2^\kappa} + t^{2^\eta} + 1$$

also impossible. This completes the proof.

Lemma 6.5. *Up to permutations, the set S_{31} of (k, h, l) in $\mathbf{N}_0^3$ such that*

$$u(k) + u(h) + u(l) = 1$$

is the union of

$$\{(k, k, 2^\lambda);\ k, \lambda = 0, 1, 2, \ldots\}, \tag{6.5.1}$$

$$\{(2^\kappa, 2^\eta, 2^\lambda);\ \kappa, \eta, \lambda = 0, 1, 2, \ldots\}, \tag{6.5.2}$$

$$\{(2^\alpha + 2^\beta, 2^\beta + 2^\gamma, 2^\gamma + 2^\alpha);\ \alpha, \beta, \gamma = 0, 1, 2, \ldots\}. \tag{6.5.3}$$

Proof. Again we verify that the set $S_{31}^?$ defined by (6.5.1), (6.5.2), (6.5.3) is contained in S_{31}; here the equation

$$u(2^\alpha + 2^\beta) = 1 + t^{2^\alpha} + t^{2^\beta} \tag{6.6}$$

(which implies Lemma 6.1 for $\omega = 2$ if $\alpha \neq \beta$) is helpful. We again proceed by induction to prove the opposite inclusion.

If k, h, l are all even then we proceed via $\frac{1}{2}(k, h, l)$ as above.

If k, h are even and l is odd then differentiation gives $l = 1$. Then (k, h) lies in the set S_2 of Lemma 6.2. If $k = h$ then we are in (6.5.1), and if $k = 2^\kappa,\ h = 2^\eta$ then in (6.5.2). Similar arguments work if exactly two of k, h, l are even.

If l is even and k, h are odd then differentiation shows that now $(k - 1, h - 1)$ lies in S_2. The case $k - 1 = h - 1$ leads to $l = 2^\lambda$ and so (6.5.1). The other case $k - 1 = 2^\kappa,\ h - 1 = 2^\eta$ leads to

$$1 = u(k) + u(h) + u(l) = t^{2^\kappa} + t^{2^\eta} + u(l).$$

So by Lemma 6.1 we have $2^{\omega(l)} - 1 = 1$ or 3. The first case gives $l = 2^\lambda,\ k = h$ and again we are in (6.5.1). The second case gives $\omega(l) = 2$ so $l = 2^\gamma + 2^\alpha$. But then (6.6) shows that $\{\kappa, \eta\} = \{\gamma, \alpha\}$. Thus we land in the new type of set (6.5.3) with $\beta = 0$. Similar arguments work if exactly one of k, h, l is even.

Finally if k, h, l are all odd then we get $(k - 1, h - 1, l - 1)$ in the set S_3 of Lemma 6.4 so in (6.4.1) or (6.4.2). The first leads to $k = h,\ l = 1$ so (6.5.1). The second leads to $k = 2^\kappa + 1,\ h = 2^\eta + 1,\ l = 1$ and now

$$1 = u(k) + u(h) + u(l) = t^{2^\kappa} + t^{2^\eta} + 1$$

forcing $k = h$ and so also (6.5.1). This completes the proof.

Lemma 6.6. *Up to permutations of k, h and of l, j, the set S_{2tt} of (k, h, l, j) in $\mathbf{N}_0^4$ such that*

$$u(k) + u(h) + t^l + t^j = 0$$

is the union of

$$\{(k, k, l, l);\ k, l = 0, 1, 2, \ldots\}, \tag{6.6.1}$$

$$\{(2^\kappa, 2^\eta, l, l);\ \kappa, \eta, l = 0, 1, 2, \ldots\}, \tag{6.6.2}$$

$$\{(2^\lambda + 2^\theta, 2^\eta, 2^\lambda, 2^\theta);\ \eta, \lambda, \theta = 0, 1, 2, \ldots\}, \tag{6.6.3}$$

$$\{(2^\lambda + 2^\alpha, 2^\theta + 2^\alpha, 2^\lambda, 2^\theta);\ \alpha, \lambda, \theta = 0, 1, 2, \ldots\}. \tag{6.6.4}$$

Proof. The usual strategy with $S^?_{2tt}$ defined by the four sets above. But due to less symmetry and more variables there are uncomfortably many parity cases to consider.

If k, h, l, j are all even then we proceed via $\frac{1}{2}(k, h, l, j)$ as above.

If k, l, j are even and h is odd then differentiation gives $h = 1$ so

$$0 = u(k) + u(h) + t^l + t^j = u(k) + 1 + t^l + t^j.$$

Thus $2^{\omega(k)} - 1 = 1$ or 3. The first case gives $k = 2^\kappa$ and then $l = j$ so we are in (6.6.2). The second case gives $k = 2^\alpha + 2^\beta$ and then by (6.6) we see that $\{l, j\} = \{2^\alpha, 2^\beta\}$ so we are in (6.6.3).

If k, h, l are even and j is odd then differentiation gives a contradiction. This covers all cases when exactly three of k, h, l, j are even.

Next suppose that l, j are even and k, h are odd. We deduce that $(k - 1, h - 1)$ is in the set S_2 of Lemma 6.2. If $k - 1 = h - 1$ then at once $l = j$ and we land in (6.6.1). Otherwise $k = 2^\kappa + 1,\ h = 2^\eta + 1$ and then

$$0 = u(k) + u(h) + t^l + t^j = t^{2^\kappa} + t^{2^\eta} + t^l + t^j.$$

Now $l = j$ implies $k = h$ so again (6.6.1); and $l = 2^\kappa,\ j = 2^\eta$ lands in (6.6.4).

Next suppose that k, h are even and l, j are odd. We deduce that $l = j$ so (k, h) is in S_2. If $k = h$ we are in (6.6.1) and if $k = 2^\kappa,\ h = 2^\eta$ we are in (6.6.2).

The remaining case when exactly two of k, h, l, j are even is essentially with h, j even and k, l odd. This leads to $u(k - 1) + t^{l-1} = 0$ so $2^{\omega(k-1)} - 1 = 1$ and $k = 2^\kappa + 1,\ l = 1$. So

$$0 = u(k) + u(h) + t^l + t^j = 1 + t^{2^\kappa} + u(h) + t^j. \tag{6.7}$$

Therefore $2^{\omega(h)} - 1 = 1$ or 3 and $\omega(h) = 1$ or 2. In the first case $h = 2^\eta,\ j = 2^\kappa$ and we land in (6.6.3). Otherwise $h = 2^\theta + 2^\alpha$ with $2^\theta \neq 2^\alpha$ and it follows from (6.6) and (6.7) that $\{2^\kappa, j\} = \{2^\theta, 2^\alpha\}$. Now we land in (6.6.4).

Next suppose j is even and k, h, l are odd. Then $(k - 1, h - 1, l - 1)$ is in the set S_{2t} of Lemma 6.3. We can assume that $h = l = 1$ and $k = 2^\kappa + 1$. Then

$$0 = u(k) + u(h) + t^l + t^j = t^{2^\kappa} + t^j$$

so $j = 2^\kappa$ and we are in (6.6.3).

Next suppose k is even and h, l, j are odd, so that $u(h - 1) + t^{l-1} + t^{j-1} = 0$. This forces $2^{\omega(h-1)} - 1 = 0,\ h = 1,\ l = j$. Now

$$0 = u(k) + u(h) + t^l + t^j = u(k) + 1$$

so $k = 2^\kappa$ and we are in (6.6.2). This covers all cases with exactly one of k, h, l, j being even.

Finally if k, h, l, j are all odd then we get $(k - 1, h - 1, l - 1, j - 1)$ in S_{2tt} so in (6.6.1), (6.6.2), (6.6.3) or (6.6.4).

If $(k - 1, h - 1, l - 1, j - 1)$ is in (6.6.1) then (k, h, l, j) too and we are done.

If in (6.6.2) then $k = 2^\kappa + 1,\ h = 2^\eta + 1,\ l = j$ and then

$$0 = u(k) + u(h) + t^l + t^j = t^{2^\kappa} + t^{2^\eta}$$

forces $k = h$ so we land in (6.6.1) again.

If in (6.6.3) then we can assume

$$k = 2^\lambda + 2^\theta + 1, \qquad h = 2^\eta + 1, \qquad l = 2^\lambda + 1, \qquad j = 2^\theta + 1.$$

Now using

$$u(1+2^\lambda+2^\theta) = 1+t+t^{2^\lambda}+t^{2^\theta}+t^{2^\lambda+1}+t^{2^\theta+1}+t^{2^\lambda+2^\theta} \tag{6.8}$$

we calculate

$$0 = u(k)+u(h)+t^l+t^j = t^{2^\lambda}+t^{2^\theta}+t^{2^\eta}+t^{2^\lambda+2^\theta}.$$

This forces $2^\eta = 2^\lambda + 2^\theta$. And then $\lambda = \theta,\ \eta = \theta+1$, which brings us into (6.6.1).

Finally if in (6.6.4) then we can assume

$$k = 2^\lambda + 2^\alpha + 1, \qquad h = 2^\theta + 2^\alpha + 1, \qquad l = 2^\lambda + 1, \qquad j = 2^\theta + 1$$

and now

$$0 = u(k)+u(h)+t^l+t^j = t^{2^\lambda}+t^{2^\theta}+t^{2^\lambda+2^\alpha}+t^{2^\theta+2^\alpha}.$$

This forces $\lambda = \theta$ and so (6.6.1). The proof is at last complete.

We can now establish Theorem 3′, continuing our usual strategy but with the relief of total symmetry. Write S_4 for the set of all solutions, which using (6.6) we can verify to contain (6.1)–(6.5).

If k, h, l, j are all even then we proceed via $\frac{1}{2}(k, h, l, j)$.

If k, h, l are even and j is odd then at once $j = 1$ and then (k, h, l) lies in the set S_{31} of Lemma 6.5, so in one of (6.5.1)–(6.5.3). If in (6.5.1) then $(k, h, l, j) = (k, k, 2^\lambda, 1)$ is in (6.2). If in (6.5.2) then $(k, h, l, j) = (2^\kappa, 2^\eta, 2^\lambda, 1)$ and we land in (6.3). And if in (6.5.3) then we land in (6.4).

If l, j are even and k, h are odd then we find that $(k-1, h-1)$ lies in S_2, so there are two cases (6.2.1), (6.2.2). The first gives $k = h$, and now (l, j) is also in S_2. This leads to (6.1) or (6.2). The second gives $k = 2^\kappa + 1,\ h = 2^\eta + 1$ so that

$$0 = u(k)+u(h)+u(l)+u(j) = t^{2^\kappa}+t^{2^\eta}+u(l)+u(j)$$

and so $(l, j, 2^\kappa, 2^\eta)$ is in the set S_{2tt} of Lemma 6.6, leading to four cases.

If $(l, j, 2^\kappa, 2^\eta)$ is in (6.6.1) then we land in (6.1).

If in (6.6.2) then $l = 2^\lambda,\ j = 2^\theta$ and $\kappa = \eta$ and we land in (6.2).

If in (6.6.3) then $l = 2^\kappa + 2^\eta,\ j = 2^\theta$ and we land in (6.4).

If in (6.6.4) then $l = 2^\kappa + 2^\alpha,\ j = 2^\eta + 2^\alpha$ and we land in (6.5). This covers all cases with exactly two of k, h, l, j being even.

Suppose now that j is even and k, h, l are odd. We find that $(k-1, h-1, l-1)$ is in the set S_3 of Lemma 6.4, leading to the cases (6.4.1), (6.4.2).

If (6.4.1) then $k = h,\ l = 1$ and we get $u(j) = 1$ so $j = 2^\theta$, landing in (6.2).

If (6.4.2) then $k = 2^\kappa + 1,\ h = 2^\eta + 1,\ l = 1$ and we get

$$0 = u(k)+u(h)+u(l)+u(j) = t^{2^\kappa}+t^{2^\eta}+1+u(j)$$

so $2^{\omega(j)} - 1 = 1$ or 3. Thus either $j = 2^\theta,\ k = h$ leading to (6.2), or $j = 2^\alpha + 2^\beta$ with $2^\alpha \neq 2^\beta$ so that $t^{2^\kappa}+t^{2^\eta}+t^{2^\alpha}+t^{2^\beta} = 0$. This forces $\{2^\kappa, 2^\eta\} = \{2^\alpha, 2^\beta\}$ leading to (6.4).

Finally if k, h, l, j are all odd then we get $(k-1, h-1, l-1, j-1)$ in S_4 so by induction in (6.1), (6.2), (6.3), (6.4) or (6.5). (The proof is soon over.)

If in (6.1) then we get at once (6.1) also for (k, h, l, j).

If in (6.2) then $k = h$ so (l, j) is in S_2 and by Lemma 6.2 we land in (6.1) or (6.2).

If in (6.3) then we get $t^{2^\kappa} + t^{2^\eta} + t^{2^\lambda} + t^{2^\theta} = 0$ which leads to (6.1) again.

If in (6.4) then we find using (6.8) the equation

$$t^{2^\alpha+2^\beta} + t^{2^\beta+2^\gamma} + t^{2^\gamma+2^\alpha} + t^{2^\theta} = 0.$$

So the exponents are equal in pairs, which implies that two of α, β, γ are equal. We may assume $\alpha = \gamma$, and then $k = h$, so (l, j) is in S_2 and we land again in either (6.1) or (6.2).

Really finally if in (6.5) then we get in a similar way

$$t^{2^\alpha+2^\gamma} + t^{2^\beta+2^\gamma} + t^{2^\alpha+2^\delta} + t^{2^\beta+2^\delta} = 0.$$

Now for example $2^\alpha + 2^\gamma = 2^\beta + 2^\gamma$ gives $\alpha = \beta$ so again $k = h$ and (l, j) in S_2 leading as above to (6.1) or (6.2). Similarly for $2^\alpha + 2^\gamma = 2^\alpha + 2^\delta$. But what about $2^\alpha + 2^\gamma = 2^\beta + 2^\delta$? Then we must also have $2^\beta + 2^\gamma = 2^\alpha + 2^\delta$ and these two equations lead again to $\alpha = \beta$ and the same conclusion.

This completes the proof of Theorem 3′ and so of Theorem 3.

Appendix A

Here we show that the bounds $d - 2$ in Theorems B1 and B2 are best possible for each $d \geq 2$.

In the following we assume $d \geq 3$, although the construction works fine for $d = 2$ with the obvious interpretations. Choose any prime $p \geq d$, and define the recurrence

$$u(k) = \sum_{r=0}^{d-1} (-1)^r \binom{d-1}{r} (t + r)^k$$

of order at most d over $\mathbf{F}_p(t)$. We claim that it vanishes on the elementary p-nested set $D_p(0; c_1, \ldots, c_g)$ in $\mathbf{Z}$ with $g = d - 2$ and $c_1 = \cdots = c_g = 1$; in other words, at all $k = q_1 + \cdots + q_{d-2}$, where $q_1, \ldots, q_{d-2}$ are any powers of p. In fact then

$$u(k) = \sum_{r=0}^{d-1} (-1)^r \binom{d-1}{r} \prod_{i=1}^{d-2} (t + r)^{q_i} = \sum_{r=0}^{d-1} (-1)^r \binom{d-1}{r} \prod_{i=1}^{d-2} (t^{q_i} + r).$$

Expanding the product here as a sum of powers r^m of r, we see that $u(k)$ is a linear combination of terms

$$u_m = \sum_{r=0}^{d-1} (-1)^r \binom{d-1}{r} r^m \quad (m = 0, 1, \ldots, d - 2).$$

Now u_m for any m is the value at $x = 1$ of the function

$$\left(x \frac{\mathrm{d}}{\mathrm{d}x}\right)^m \sum_{r=0}^{d-1} (-1)^r \binom{d-1}{r} x^r = \left(x \frac{\mathrm{d}}{\mathrm{d}x}\right)^m (1 - x)^{d-1} \tag{A.1}$$

which is clearly zero for $m = 0, 1, \ldots, d - 2$. This proves the claim above.

We next check that u is not identically zero on $\mathbf{N}_0$. By the above observation

$$u(d-1) = \sum_{r=0}^{d-1} (-1)^r \binom{d-1}{r} (t + r)^{d-1} = \sum_{m=0}^{d-1} \binom{d-1}{m} t^{d-1-m} u_m = u_{d-1}.$$

Expanding $\left(x\frac{\mathrm{d}}{\mathrm{d}x}\right)^{d-1} = x^{d-1}\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^{d-1} + \cdots$ in (A.1), we see that u_{d-1} is the value at $x = 1$ of $x^{d-1}\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^{d-1}(1-x)^{d-1}$. This is $(-1)^{d-1}(d-1)! \neq 0$ because $p \geq d$.

Now we show that the zero set $\mathcal{Z}$ in $\mathbf{N}_0$ of u cannot be p-normal of order less than $d-2$; for this we use counting considerations as in [7] (p. 179). Since $p \geq d$ it is obvious that u is simple and non-degenerate in the sense of [7] (p. 182). Thus by Theorem 2.7 of [7] (p. 184) $\mathcal{Z}$ cannot contain an infinite arithmetic progression. If now it were p-normal of order less than $d-2$ it would follow from Corollary 1.11 of [7] (p. 179) that the number of its elements with absolute value at most B has order of magnitude at most $(\log B)^{d-3}$ as $B \to \infty$. But already the number of elements in $D_p(0; c_1, \ldots, c_g)$ above clearly has order at least $(\log B)^{d-2}$ as $B \to \infty$. This verifies that Theorem B2 is indeed best possible; and a similar argument works for Theorem B1.

We may remark that it now follows from [7] that u cannot have order less than d (this could of course be proved directly). So the order is exactly d.

Appendix B

To prove the Cerlienco–Mignotte–Piras Conjecture in zero characteristic, we start with the following probably well-known observation.

Lemma. *Given positive integers n, d and independent variables $x_1, \ldots, x_n$ there are $M = \binom{n+d}{n}$ polynomials $X_1, \ldots, X_M$ in $\mathbf{Q}[x_1, \ldots, x_n]$ of total degree at most 1 with*

$$\mathbf{Z} + \mathbf{Z}x_1 + \cdots + \mathbf{Z}x_n = \mathbf{Z}X_1 + \cdots + \mathbf{Z}X_M \tag{B.1}$$

such that every monomial $x_1^{d_1} \cdots x_n^{d_n}$ of total degree at most d lies in $\mathbf{Q}X_1^d + \cdots + \mathbf{Q}X_M^d$.

Proof. It is certainly well-known that a generic set of M points in $\mathbf{C}^n$ lies in no hypersurface of degree at most d; we get M homogeneous linear equations for the M coefficients defining the hypersurface, and in general the determinant does not vanish. Thus this holds for some set of M points π in $\mathbf{Q}^n$ (in fact it holds for the special set of integer points $(\xi_1, \ldots, \xi_n)$ with non-negative coordinates satisfying $\xi_1 + \cdots + \xi_n \leq d$, although we could not find a reference). By a translation we can suppose that one of the points is the origin, and then the remaining points cannot lie on a hyperplane through the origin so by a linear transformation we can also suppose that they include the standard basis vectors of $\mathbf{Q}^n$. Thus defining the vector $\mathbf{v}(\pi)$ with M components $\xi_1^{d_1} \cdots \xi_n^{d_n}$ $(d_1 + \cdots + d_n \leq d)$, we get $\pi_1, \ldots, \pi_M$ in $\mathbf{Z}^n$ with $\mathbf{v}(\pi_1), \ldots, \mathbf{v}(\pi_M)$ linearly independent. Now putting $X(\pi) = 1 + \xi_1 x_1 + \cdots + \xi_n x_n$ and $X_i = X(\pi_i)$ $(i = 1, \ldots, M)$ we deduce that $X_1^d, \ldots, X_M^d$ are themselves linearly independent. They therefore span the whole space of polynomials of total degree at most d. And (B.1) holds because already we can choose $X_1 = 1 + x_1, \ldots, X_n = 1 + x_n$ and $X_M = 1$, so that $x_j = X_j - X_M$ $(j = 1, \ldots, n)$. This completes the proof.

Now Matijasevich proved (see for example [14] quoted below for references) that there is a universal diophantine equation, say in n variables $x_1, \ldots, x_n$ with total degree $d \geq 2$ and some additional parameters. This implies that one can specialize some parameters to obtain a polynomial $P(\mathbf{t}; x_1, \ldots, x_n)$ representing a family of undecidable diophantine equations with respect to the parameters in $\mathbf{t}$. We change the variables to $X_1, \ldots, X_M$ as in the Lemma, so that we can write

$$P(\mathbf{t}; x_1, \ldots, x_n) = p_1(\mathbf{t})X_1^d + \cdots + p_M(\mathbf{t})X_M^d$$

with polynomials $p_1(\mathbf{t}), \ldots, p_M(\mathbf{t})$ in $\mathbf{Q}[\mathbf{t}]$. Of course $M > n+1$ and so the new variables are not independent, and there will be non-zero $\mathbf{a} = (a_1, \ldots, a_M)$ in $\mathbf{Q}^M$ such that

$$L(\mathbf{a}; X_1, \ldots, X_M) = a_1 X_1 + \cdots + a_M X_M = 0.$$

However we can pick basis elements $\mathbf{a}_1, \ldots, \mathbf{a}_N$ of the space of such $\mathbf{a}$ (including $\mathbf{a} = 0$). Thanks to (B.1) the solvability of

$$\begin{aligned} &p_1(\mathbf{t})X_1^d + \cdots + p_M(\mathbf{t})X_M^d = 0, \\ &L(\mathbf{a}_1; X_1, \ldots, X_M) = 0, \ldots, L(\mathbf{a}_N; X_1, \ldots, X_M) = 0 \end{aligned} \tag{B.2}$$

in integers $X_1, \ldots, X_M$ is equivalent to the solvability of $P(\mathbf{t}; x_1, \ldots, x_n) = 0$ in integers $x_1, \ldots, x_n$. But the system (B.2) is diagonal.

Now the standard trick with sums of squares to reduce a system to a single equation will probably destroy the diagonal property. Instead we pick algebraic $\theta_1, \ldots, \theta_N$ with $1, \theta_1, \ldots, \theta_N$ linearly independent over $\mathbf{Q}$ and take the appropriate linear combination of (B.2); compare (1.5). This yields a diagonal equation

$$P_1(\mathbf{t}; X_1) + \cdots + P_M(\mathbf{t}; X_M) = 0$$

(and in fact each $P_i(X)$ has the shape $pX^d + \alpha X + \beta$). Thus indeed (1.4) is undecidable with $m = M$; and since $X_M = 1$ in the proof of the Lemma we could even take $m = M - 1$.

Finally according to Theorem 4 (p. 552) of the paper [14] of J.P. Jones we can choose $n = 58$, $d = 4$ giving $M = \binom{62}{58} = 557845$ and so $m = 557844$.

Acknowledgment

The first author was partially supported by NSF grant DMS 1302032.

References

[1] B. Adamczewski, J. Bell, On vanishing coefficients of algebraic power series over fields of positive characteristic, Invent. Math. 187 (2012) 343–393.
[2] F. Amoroso, E. Viada, Small points on subvarieties of a torus, Duke Math. J. 150 (2009) 407–442.
[3] L. Arenas-Carmona, D. Berend, V. Bergelson, Ledrappier's system is almost mixing of all orders, Ergodic Theory Dynam. Systems 28 (2008) 339–365.
[4] F. Beukers, The multiplicity of ternary sequences, Compos. Math. 77 (1991) 165–177.
[5] Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential diophantine equations I, Ann. of Math. 163 (2006) 969–1018.
[6] L. Cerlienco, M. Mignotte, F. Piras, Suites récurrentes linéaires, Enseign. Math. 33 (1987) 67–108.
[7] H. Derksen, A Skolem-Mahler-Lech theorem in positive characteristic and finite automata, Invent. Math. 168 (2007) 175–224.
[8] H. Derksen, D. Masser, Linear equations over multiplicative groups, recurrences, and mixing I, Proc. Lond. Math. Soc. 104 (2012) 1045–1083.
[9] H. Derksen, D. Masser, Linear equations over multiplicative groups, recurrences, and mixing III, in preparation.
[10] G. Everest, A.J. van der Poorten, I. Sparlinski, T. Ward, Recurrence sequences, in: Math. Surveys and Monographs, vol. 104, American Math. Soc, 2003.
[11] J.-H. Evertse, On sums of S-units and linear recurrences, Compos. Math. 53 (1984) 225–244.
[12] J.-H. Evertse, H.P. Schlickewei, W.M. Schmidt, Linear equations in variables which lie in a multiplicative group, Ann. of Math. 155 (2002) 807–836.
[13] D. Goss, Basic structures of function field arithmetic, in: Ergebnisse der Math., vol. 35, Springer, 1996.
[14] J.P. Jones, Universal diophantine equation, J. Symbolic Logic 47 (1982) 549–571.
[15] M. Laurent, Équations exponentielles-polynômes et suites récurrentes linéaires, Astérisque 147–148 (1987) 121–139.

[16] M. Laurent, Équations exponentielles-polynômes et suites récurrentes linéaires, II, J. Number Theory 31 (1989) 24–53.
[17] F. Ledrappier, Un champ markovien peut être d'entropie nulle et mélangeant, C. R. Acad. Sci. Paris A287 (1978) 561–562.
[18] D. Leitner, Linear equations over multiplicative groups in positive characteristic, Acta Arith. 153 (2012) 325–347.
[19] V. Losert, The set of solutions of some equation for linear recurrence sequences, in: H.P. Schlickewei, K. Schmidt, R.F. Tichy (Eds.), Diophantine Approximation, vol. 16, Springer Developments in Math, 2008, pp. 231–235.
[20] D. Masser, Mixing and linear equations over groups in positive characteristic, Israel J. Math. 142 (2004) 189–204.
[21] H.P Schlickewei, W.M. Schmidt, Equations $au_n^l = bu_m^k$ satisfied by members of recurrence sequences, Proc. Amer. Math. Soc. 118 (1993) 1043–1051.
[22] H.P. Schlickewei, W.M. Schmidt, Linear equations in members of recurrence sequences, Ann. Scuola Norm. Sup. Pisa 20 (1993) 219–246.
[23] H.P. Schlickewei, W.M. Schmidt, The intersection of recurrence sequences, Acta Arith. LXXII (1995) 1–44.
[24] H.P. Schlickewei, W.M. Schmidt, The number of solutions of polynomial-exponential equations, Compos. Math. 120 (2000) 193–225.
[25] W.M. Schmidt, Linear recurrence sequences, in: F. Amoroso, U. Zannier (Eds.), Diophantine Approximation, in: Springer Lectures Notes, vol. 1819, 2003, pp. 171–247.
[26] W.M. Schmidt, Zeros of linear recurrence sequences, Publ. Math. Debrecen 56 (2000) 609–630.