Effective difference elimination and Nullstellensatz

Alexey Ovchinnikov　　　　Gleb Pogudin　　　　Thomas Scanlon

Abstract

We prove effective Nullstellensatz and elimination theorems for difference equations in sequence rings. More precisely, we compute an explicit function of geometric quantities associated to a system of difference equations (and these geometric quantities may themselves be bounded by a function of the number of variables, the order of the equations, and the degrees of the equations) so that for any system of difference equations in variables $\mathbf{x} = (x_1, \ldots, x_m)$ and $\mathbf{u} = (u_1, \ldots, u_r)$, if these equations have any nontrivial consequences in the $\mathbf{x}$ variables, then such a consequence may be seen algebraically considering transforms up to the order of our bound. Specializing to the case of $m = 0$, we obtain an effective method to test whether a given system of difference equations is consistent.

Keywords. difference equations, effective Nullstellensatz, elimination of unknowns

1 Introduction

Let K be an algebraically closed field of arbitrary characteristic. We say that a sequence $(a_j)_{j=0}^{\infty}$ from K satisfies a difference equation with constant coefficients if there is a nonzero polynomial $F(x_0, \ldots, x_e) \in K[x_0, \ldots, x_e]$ such that, for every natural number j, the equation $F(a_j, a_{j+1}, \ldots, a_{j+e}) = 0$ holds. This can also be defined for systems of difference equations in several variables. Such difference equations and the sequences that solve them are ubiquitous throughout mathematics and in its applications to the sciences, including such areas as combinatorics, number theory, control theory, and epidemiology, amongst many others (see Section 4 for some of the examples).

In this paper we resolve some fundamental problems about difference equations. The questions we answer include the following (for precise statements, including the way non-constant coefficients can appear, see Section 3):

1. Under what conditions does a system of difference equations have a sequence solution?

2. Can these conditions be made sufficiently transparent to allow for efficient computation?

3. Given a system of difference equations on $(n + m)$-tuples of sequences, how does one eliminate some of the variables so as to deduce the consequences of these equations on the first n variables?

Our solution to the first question is a conceptual difference Nullstellensatz, to the second, an effective difference Nullstellensatz, and to the third, an effective difference elimination algorithm. Even though the abstract Nullstellensatz is intellectually satisfying in that conditions of different kinds are shown to be equivalent, namely the existential condition that there is a sequence solution to a system of difference equations and the universal condition that the difference ideal generated by the equations is proper, the difficult work and applications, both theoretical and practical, comes with our main effective theorems.

Effective elimination theorems and methods have a long history and play central roles in computational algebra. Row reduction, or Gaussian elimination, is a fundamental technique in linear algebra. Elimination for polynomial equations is substantially more complicated and has been the subject of intensive and sophisticated work [4, 23, 22]. In recent work of the first two authors joined by Vo [29], effective elimination theorems were obtained for algebraic differential equations through a reduction to the polynomial case through the decomposition-elimination-prolongation method. Elimination of unknowns for systems of linear difference equations is an essential part of the classical transfer matrix method in combinatorics [34, §4.7].

While these questions are important and difference equations have been studied intensively both for their applications and theory, to our knowledge, none of these questions has received a satisfactory answer in the literature. We explain below how some known results, both positive and negative, may help explain the existence of this lacuna. In particular, in some essential ways, the effective Nullstellensatz and elimination problems for difference equations are substantially more difficult than the corresponding problems for differential equations and the methods of [29] do not routinely transpose to this context.

The foundational work on difference algebra, that is, the study of the theory of difference rings and of difference equations as encoded through the algebraic properties of rings of difference polynomials, was initiated by Cohn in [6], following the tradition

of Ritt and Kolchin in differential algebra. Deep results have been obtained in this subject, but their relevance to the problems at hand is hampered by their restrictions, for the Nullstellensatz and elimination theorems, to the case in which solutions are sought in difference *fields*, and thus have little bearing on the structures used in practice, namely difference rings presented as rings of sequences, such as $\mathbb{C}^{\mathbb{N}}$ given with the shift operator $\sigma : (a_i)_{i=0}^{\infty} \mapsto (a_{i+1})_{i=0}^{\infty}$. Moreover, even if restricted to difference fields, the known elimination theorems are at best theoretically effective.

Chatzidakis and Hrushovski studied difference fields from the perspective of mathematical logic in [5]. There, they established a recursive axiomatization for the theory of existentially closed difference fields and proved a quantifier simplification theorem. From this it follows that in principle there are effective procedures to check the consistency of difference equations in difference fields and to perform difference elimination in difference fields. More recent work of Tomašić [36, 37] geometrizes the quantifier simplification theorem and brings the complexity of these algorithms to primitive recursive, though this effectivity is still theoretical — to call the implicit bounds astronomical would be a gross understatement — and a practical implementation of this work is infeasible. In symbolic computation, steps have been taken towards extending the characteristic set method from differential algebra to the study of difference and difference-differential equations in works of Gao, van der Hoeven, Li, Yuan, Zhang [14, 13, 27, 26]. These methods are more efficient than those coming from logic, but as they are restricted to the study of inversive prime difference ideals, they, too, are fundamentally results about solutions to difference equations in difference fields and the constructions of difference resultants depend on restrictive hypotheses. A similar approach was taken by Lyzell, Glad, Enqvist, Ljung [28] aiming at solving a problem in discrete-time control theory.

The situation for difference equations in sequence rings differs starkly. Simple examples show that consistency checking in difference fields is not the same problem as consistency checking for sequences. For example, the system of difference equations $x\sigma(x) = 0$, $x + \sigma(x) = 1$ has no solution in a difference field, but the sequence $0, 1, 0, 1, \ldots$ is a solution in $\mathbb{C}^{\mathbb{N}}$.

More seriously, theorems of Hrushovski and Point [21] show that the logical methods used for difference fields fail dramatically for sequence rings. In particular, they show that the first-order theory of $\mathbb{C}^{\mathbb{N}}$ regarded as a difference ring is undecidable. Thus, we cannot derive a consistency checking method from a recursive axiomatization of this theory nor can we produce an elimination algorithm from an effective quantifier elimination theorem; no such axiomatization or quantifier elimination procedure exists. That we succeed in solving the effective consistency checking and effective elimination problems for difference equations in sequence rings is all the more surprising given these undecidability results.

Let us explain more precisely what we actually prove and where the new ideas appear in our arguments. We have two main theorems: Theorem 3.1 an effective Nullstellensatz and Theorem 3.4 an effective difference elimination theorem. Strictly speaking, the effective Nullstellensatz is a special case of an effective elimination theorem, but we prove elimination by bootstrapping through the Nullstellensatz.

The key to our work is a new proof technique based on the spirit of the decomposition-elimination-prolongation (DEP) method. As is completely standard, a system of difference equations may be regarded as a system of algebraic equations in more variables together with specifications that certain coordinates should be obtained from others by the application of the distinguished endomorphism and the usual DEP methods allow for one to cleverly reduce questions about the original system of difference equations to questions entirely about algebraic equations. A version of the DEP method for difference equations in difference fields is employed in [19] for the purpose of computing explicit bounds in Diophantine geometric problems. This DEP method cannot work for the problems at hand as explained in Section 5. We overcome this obstacle by taking a different approach to reducing the question about the original system to the question about algebraic equations. The core of this reduction is for us to show that every system of difference equations that has a solution actually has what we call a skew-periodic solution with the components being (not necessarily closed!) points of the affine variety corresponding to the original system, and the length of the period can be bounded in terms of the geometric data of the original system (see Section 6.2.3).

With our theorems we explicitly bound the number of prolongations required to solve the problems at hand, *i.e.* testing a system of difference equations for consistency or computing a nontrivial element of the elimination ideal. For the elimination problem, our bound is not sensitive to the number of variables that are not being eliminated, see Remark 3.6. The bounds are small enough in many cases to permit efficient computation, see Section 4.

We draw an interesting theoretical conclusion from our work towards the explicit bounds for the difference elimination problem in Section 7. Specifically, with Theorem 7.1, we show that for (K, σ) any algebraically closed difference field, whenever a finite system of difference equations over K is consistent in the sense that it has a solution in some difference ring, then it already has a solution in the ring of sequences of elements of K. We give a soft proof of such a difference Nullstellensatz under the hypothesis that K is uncountable with Proposition 6.3. The proof of Theorem 7.1 is much more difficult than it may have been expected to be. In extending this difference Nullstellensatz to general K we use crucially our result that a system of difference equations is consistent if and only if it has a skew-periodic solution and then appeal to remarkable theorems of Hrushovski on the first-order theory of the Frobenius automorphism and of Varshavsky

on intersections of correspondences with the graph of the Frobenius.

The paper is organized as follows. We give the basic definitions in Section 2, and then introduce the notation and terminology specific to our paper. The main results, Theorem 3.1 for the effective Nullstellensatz and Theorem 3.4 for the effective elimination, are expressed in Section 3. In Section 4, we illustrate our results in several practical examples. With Section 5, we present counterexamples to an effective strong difference Nullstellensatz and to the application of the usual DEP method to these problems. The proofs of the main theorems are presented in Section 6. Finally, in Section 7, we strengthen the difference Nullstellensatz giving equivalent criteria for the existence of sequence solutions to systems difference equations over any algebraically closed field.

2 Preliminaries

Throughout the paper, $\mathbb{N}$ denotes the set of non-negative integers. A detailed introduction to difference rings can be found in [6, 25].

Definition 2.1 (Difference rings)**.**

- A *difference ring* is a pair (A, σ) where A is a commutative ring and $\sigma : A \to A$ is a ring endomorphism.

- As an example, if R is any commutative ring, then the sequence rings $R^{\mathbb{N}}$ and $R^{\mathbb{Z}}$ are difference rings with σ defined by $\sigma((x_i)_{i \in \mathbb{N}}) := (x_{i+1})_{i \in \mathbb{N}}$ ($\sigma((x_i)_{i \in \mathbb{Z}}) := (x_{i+1})_{i \in \mathbb{Z}}$, respectively).

- A *map of difference rings* $\psi : (A, \sigma) \to (B, \tau)$ is given by a map of rings $\psi : A \to B$ such that that $\tau \circ \psi = \psi \circ \sigma$.

- We often abuse notation saying that A is a difference ring when we mean the pair (A, σ).

Definition 2.2 (Difference polynomials)**.** Let A be a difference ring.

- The free difference A-algebra in one generator x over A, $A\{x\}$, also called the *ring of difference polynomials* in x over A, may be realized as the ordinary polynomial ring $A[\{\sigma^j(x) \ : \ j \in \mathbb{N}\}]$ in the indeterminates $\{\sigma^j(x) \ : \ j \in \mathbb{N}\}$.

- Iterating this procedure, one obtains the difference polynomial ring $A\{x_1, \ldots, x_n\}$ in n variables.

- Every difference polynomial in $A\{x_1, \ldots, x_n\}$ can be considered as an ordinary polynomial in indeterminates of the form $\sigma^i(x_j)$.

- For $P \in A\{x_1, \ldots, x_n\}$ and $1 \leqslant i \leqslant n$, we define the *order* of P with respect to x_i, denoted $\mathrm{ord}_{x_i}(P)$ to be the maximal h for which $\sigma^h(x_i)$ appears in P. If no $\sigma^h(x_i)$ appears, we set $\mathrm{ord}_{x_i}(P) := -1$. We also set $\mathrm{ord}\, P := \max\limits_{1 \leqslant i \leqslant n} \mathrm{ord}_{x_i} P$.

Example 2.3. $\mathrm{ord}_{x_3}(\sigma^3(x_1) + x_2 + \sigma(x_3)^2 + 1)$=1.

Definition 2.4. If (A, σ) is a difference ring and $F \subseteq A\{x_1, \ldots, x_n\}$ is a set of difference polynomials over A, $(A, \sigma) \subseteq (B, \sigma)$ is an extension of difference rings, and $\mathbf{b} = (b_1, \ldots, b_n) \in B^n$ is an n-tuple from B, then we say that $\mathbf{b}$ is a *solution* of the system $F = 0$ if, under the unique map of difference rings $A\{x_1, \ldots, x_n\} \to B$ given by extending the given map $A \to B$ and sending $x_i \mapsto b_i$ for $1 \leqslant i \leqslant n$, every element of F is sent to 0.

Example 2.5. Let $(A, \sigma) = (\mathbb{Q}, \mathrm{id})$ and $(B, \sigma) = (\mathbb{Q}^{\mathbb{N}}, \sigma)$, where σ is the shift (to the left) operator. Then the tuple

$$\mathbf{b} = ((1, 0, 1, 0, \ldots), (2018, 1, 0, 1, \ldots)) \in B^2$$

is a solution of the system

$$\begin{cases} \sigma(x_1) + x_1 - 1 = 0, \\ \sigma(x_2) - x_1 = 0. \end{cases}$$

Definition 2.6. If (A, σ) is a difference ring, $F \subseteq A\{x_1, \ldots, x_n\}$, and B is a non-negative integer, the *B-th transform* of F is the set

$$\sigma^B(F) := \left\{ \sigma^B(f) \mid f \in F \right\}.$$

So, the 0-th transform of F is F. The B-th transform of a system of difference equations is defined similarly.

Example 2.7. The 2-nd transform of the system

$$\begin{cases} \sigma(x_1)^5 = x_1 + x_2^2 \\ x_3^3 + x_1 + 1 = 0 \end{cases}$$

is the system

$$\begin{cases} \sigma^3(x_1)^5 = \sigma^2(x_1) + \sigma^2(x_2)^2 \\ \sigma^2(x_3)^3 + \sigma^2(x_1) + 1 = 0. \end{cases}$$

The ideal generated by a set F in a commutative ring R is denoted by $\langle F \rangle$.

Definition 2.8. A difference equation $g(x_1, \ldots, x_n) = 0$ is said to be a *consequence* of a system of difference equations $F = 0$, where $F \subset k\{x_1, \ldots, x_n\}$, if there exists a non-negative integer B such that

$$g \in \left\langle \sigma^i(F) \mid 0 \leqslant i < B \right\rangle.$$

Example 2.9. Let $F = 0$ be the system

$$\begin{cases} f_1 = x_2\sigma(x_1) - x_1 - 1 = 0 \\ f_2 = \sigma(x_2) - x_2^2 = 0. \end{cases}$$

The equation $\sigma^2(x_1)x_2^2 - \sigma(x_1) - 1$ is a consequence of $F = 0$ with $B = 2$ because

$$\sigma(f_1) - \sigma^2(x_1)f_2 = \sigma(x_2\sigma(x_1) - x_1 - 1) - \sigma^2(x_1)(\sigma(x_2) - x_2^2) = \sigma^2(x_1)x_2^2 - \sigma(x_1) - 1.$$

We define the degree of an affine algebraic variety following [16, Definition 1 and Remark 2] as follows.

Definition 2.10. Let X be an irreducible affine variety of dimension r in $\mathbb{A}^n$. Then we define

$$\deg X := \max\left\{|X \cap E| \mid E \text{ is an affine subspace of } \mathbb{A}^n \text{ with } \dim E = n-r \text{ and } |X \cap E| < \infty\right\}.$$

Let X be an affine variety defined over a field k. Let $X = X_1 \cup \ldots \cup X_N$ be the decomposition of X into irreducible components over the algebraic closure of k. Then we define

$$\deg X := \sum_{i=1}^N \deg X_i.$$

3   Main results

For all $d \in \mathbb{Z}_{\geqslant 0}$ and $D \in \mathbb{Z}_{>0}$ we define

$$B(d, D) = \begin{cases} D + 1 & \text{if } d = 0, \\ \frac{D^3}{6} + \frac{D^2}{2} + \frac{4D}{3} + 1 & \text{if } d = 1, \\ B(d-1, D) + D^{B(d-1,D)} & \text{if } d > 1. \end{cases}$$

3.1   Effective difference Nullstellensatz

Theorem 3.1. *Let*

- *k be a difference field and $F = 0$ a system of difference equations, where $F := \{f_1, \ldots, f_N\} \subset k\{u_1, \ldots, u_r\}$.*

- *We set*

$$h_i := \max_{j=1,\ldots,N} \operatorname{ord}_{u_i} f_j \quad \text{and} \quad H = h_1 + \ldots + h_r + r,$$

*so, H is an upper bound on the number of the **u**-unknowns and their transforms that appear in F.*

- $d(F)$ and $D(F)$ denote the dimension and degree of the affine variety defined by F over k in the affine H-space, respectively.

The following statements are equivalent:

1. *The system $F = 0$ has a solution in a difference ring containing k;*

2. *The system $\{\sigma^i(F) = 0 \mid 0 \leqslant i < B(d, D)\}$ is consistent as a system of polynomial equations.*

Corollary 3.2. *If $k = \mathbb{C}$ in Theorem 3.1, then the following statements are equivalent:*

1. *The system $F = 0$ has a solution in $\mathbb{C}^{\mathbb{Z}}$;*

2. *The system $\{\sigma^i(F) = 0 \mid 0 \leqslant i < B(d, D)\}$ has a solution in $\mathbb{C}$ as a system of polynomial equations.*

Remark 3.3. We do not prove an effective strong Nullstellensatz generalizing Corollary 3.2, because such a statement is false as shown in Section 5.2.

3.2   Effective elimination

We will introduce the notation that will be used in Theorem 3.4.

- Let $\mathbf{x} = (x_1, \ldots, x_m)$ and $\mathbf{u} = (u_1, \ldots, u_r)$ be two sets of unknowns.

- Consider a system $F = 0$ of difference equations, where $F := \{f_1, \ldots, f_N\} \subset k\{\mathbf{x}, \mathbf{u}\}$. We would like to have an effective method for determining whether there exists a nonzero consequence of the system $F = 0$ involving only the $\mathbf{x}$-variables.

- We set
$$h_i := \max_{j=1,\ldots,N} \operatorname{ord}_{u_i} f_j \quad \text{and} \quad H = h_1 + \ldots + h_r + r,$$
so, H is an upper bound on the number of the $\mathbf{u}$-unknowns and their transforms that appear in F.

- Let E be the field of fractions of $k\{\mathbf{x}\}$ and X denote the associated affine subvariety of $\mathbb{A}^H$ defined by $F = 0$ over E. Note that X is not necessarily irreducible.

- We denote the dimension and degree of X by $d_{\mathbf{u}}(F)$ and $D_{\mathbf{u}}(F)$, respectively.

Theorem 3.4. *For all integers $d \geqslant 0$ and $D \geqslant 1$ and systems $F = 0$ in $\mathbf{x}$ and $\mathbf{u}$ with $d_{\mathbf{u}}(F) = d$ and $D_{\mathbf{u}}(F) = D$, the following statements are equivalent:*

1. *There exists a non-zero difference equation $g(\mathbf{x}) = 0$ that is a consequence of the system $F = 0$;*

2. $\langle \sigma^i(F) \mid 0 \leqslant i < B(d, D) \rangle \cap k\{\mathbf{x}\} \neq \{0\}$.

Remark 3.5. Based on the existing elimination results for differential-algebraic equations [29, Theorem 3], it is tempting to find, for a positive integer h, a bound B such that the ideal

$$\langle \sigma^i(F) \mid 0 \leqslant i < B \rangle$$

contains all the consequences of the system $F = 0$ depending only on $\mathbf{x}$-variables of order at most h. However, as we show in Section 5.3, there is no such bound in terms of degrees, orders, and the number of variables. Moreover, every such bound will depend on the coefficients of F.

Remark 3.6. The bound in Theorem 3.4 is especially small if the number of the variables to eliminate is moderate. More precisely, $d \leqslant H - 1$, and D does not exceed the product of the degrees of $H + 1$ equations of the highest degree. For particular examples, see Section 4.

3.3 Consequences for computation

Theorem 3.1 and Corollary 3.2 reduce consistency questions for systems of difference equations to consistency questions (in algebraically closed fields) of polynomial systems in finitely many variables and Theorem 3.4 reduces the question of existence/finding a consequence in the $\mathbf{x}$ variables of a system of difference equations in the variables $\mathbf{x}$ and $\mathbf{u}$ to a question about a polynomial ideal in a polynomial ring in finitely many variables. These algebraic problems are classical and have been computationally solved using, for example, Gröbner bases, triangular sets, numerical algebraic geometry, etc. For all of these methods, implementations exist in many computer algebra systems and independent software packages (see, for example, [7, 2, 35]).

4 Numerical values and practical examples

In the following table, we compute $B(d, D) - 1$ for small d and D.

$d \setminus D$	1	2	3	4	5
0	1	2	3	4	5
1		2	6	13	24	40

Remark 4.1. Almost all examples of modeling phenomena in the sciences using polynomial difference equations that we have seen in the literature can be written as systems with the same number of equations as unknowns in such a way that none of the equations is a consequence of the others. The above table is applicable to elimination problems for such systems with n equations if the problem is to eliminate $\lceil n/2 \rceil$ unknowns or less, as such

problems typically result in varieties X (see the notation of Section 3.2) of dimension 0 or 1.

Remark 4.2. One can significantly speed up checking if an elimination is possible by

1. Applying the number of transforms that is in the bound;

2. Substituting random values into the variables that are not being eliminated.

Using techniques from [29, Section 5] (see also [17]) based on the DeMillo-Lipton-Schwartz-Zippel lemma [39, Proposition 98], for each number p, $0 < p < 1$, we can find the range for the random substitution so that the probability of the elimination being possible if and only if the "substituted" system has no solutions is greater than p. So, this would give an efficient probabilistic test for the possibility of elimination.

Remark 4.3. Although there could be special tricks and methods for each of the examples below, our approach provides a general and fully automated procedure.

Example 4.4. Consider the May-Leonard model for 2-plant annual competition, scaled down from [31]:
$$\begin{cases} x_{n+1} = \frac{(1-b)x_n}{x_n + \alpha_1 y_n} + bx_n, \\ y_{n+1} = \frac{(1-b)y_n}{\alpha_2 x_n + y_n} + by_n, \end{cases}$$
which can be rewritten as
$$\begin{cases} (x + \alpha_1 y)\sigma(x) = (1-b)x + bx(x + \alpha_1 y), \\ (\alpha_2 x + y)\sigma(y) = (1-b)y + by(\alpha_2 x + y), \end{cases} \tag{4.1}$$

where $k = \mathbb{Q}(\alpha_1, \alpha_2, b)$, with σ acting as the identity on k. To verify whether y can be eliminated from (4.1), we then consider the affine variety X defined by (4.1) over the field $\mathbb{Q}(\alpha_1, \alpha_2, b, x, \sigma(x))$ with coordinates $y, \sigma(y)$. A computation shows that $d = 0$ and $D = 1$, and so $B(d, D) - 1 = 2 - 1 = 1$. A computation shows that it is not only sufficient but also necessary to apply this single transform to perform the elimination. So, our main result gives a sharp upper bound for this example.

Example 4.5. Consider the May-Leonard model for 3-plant annual competition [31]:
$$\begin{cases} x_{n+1} = \frac{(1-b)x_n}{x_n + \alpha_1 y_n + \beta_1 z_n} + bx_n, \\ y_{n+1} = \frac{(1-b)y_n}{\alpha_2 x_n + y_n + \beta_2 z_n} + by_n, \\ z_{n+1} = \frac{(1-b)z_n}{\alpha_3 x_n + \beta_3 y_n + z_n} + bz_n, \end{cases}$$
which can be rewritten as
$$\begin{cases} (x + \alpha_1 y + \beta_1 z)\sigma(x) = (1-b)x + bx(x + \alpha_1 y + \beta_1 z), \\ (\alpha_2 x + y + \beta_2 z)\sigma(y) = (1-b)y + by(\alpha_2 x + y + \beta_2 z), \\ (\alpha_3 x + \beta_3 y + z)\sigma(z) = (1-b)z + bz(\alpha_3 x + \beta_3 y + z), \end{cases} \tag{4.2}$$

where $k = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_3, \beta_3, b)$, with σ acting as the identity on k. To verify whether y and z can be eliminated from (4.2), we consider the affine variety X defined by (4.2) over the field $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_3, \beta_3, b, x, \sigma(x))$ with coordinates $y, \sigma(y), z, \sigma(z)$. A computation shows that $d = 1$ and $D = 3$, and so $B(d, D) - 1 = 13$. A computation shows that

- two prolongations are necessary and sufficient

- carrying out a computation with 13 transforms and probability $p = 0.99$ as described in Remark 4.2 to check if an elimination is possible does not take significantly more time than doing this with two transforms.

Example 4.6. Consider the stage structured Leslie-Gower model [8, eq. (5)]:

$$\begin{cases} J_{n+1} = b_1 \frac{1}{1+d_1 A_n} A_n \\ A_{n+1} = s_1 \frac{1}{1+J_n+c_1 j_n} J_n \\ j_{n+1} = b_2 \frac{1}{1+d_2 a_n} a_n \\ a_{n+1} = s_2 \frac{1}{1+c_2 J_n + j_n} j_n, \end{cases}$$

which can be rewritten as

$$\begin{cases} (1 + d_1 A)\sigma(J) = b_1 A \\ (1 + J + c_1 j)\sigma(A) = s_1 J \\ (1 + d_2 a)\sigma(j) = b_2 a \\ (1 + c_2 J + j)\sigma(a) = s_2 j, \end{cases} \tag{4.3}$$

where $k = \mathbb{Q}(b_1, b_2, c_1, c_2, d_1, d_2, s_1, s_2)$ with σ acting as the identity on k. To verify whether J and j can be eliminated from (4.3), we consider the affine variety X defined by (4.3) over the field $\mathbb{Q}(b_1, b_2, c_1, c_2, d_1, d_2, s_1, s_2, a, A, \sigma(a), \sigma(A))$ with coordinates $j, \sigma(j), J, \sigma(J)$. A computation shows that $d = 0$; $D = 1$ as the equations are linear in $j, \sigma(j), J, \sigma(J)$. Then

$$B(d, D) - 1 = 2 - 1 = 1.$$

A computation shows that it is not only sufficient but also necessary to apply this single transform to perform the elimination. So, our main result gives a sharp upper bound for this example.

Example 4.7. A discrete multi-population *SI* model from [1], similarly to the previous examples, can be rewritten as

$$\begin{cases} \sigma(S) = S\left(1 - \frac{a \cdot \Delta t}{N_1} I - \frac{b \cdot \Delta t}{N_1} i\right) \\ \sigma(s) = s\left(1 - \frac{c \cdot \Delta t}{N_2} I - \frac{d \cdot \Delta t}{N_2} i\right) \\ \sigma(I) = I + S\left(\frac{a \cdot \Delta t}{N_1} I + \frac{b \cdot \Delta t}{N_1} i\right) \\ \sigma(i) = i + s\left(\frac{c \cdot \Delta t}{N_2} I + \frac{d \cdot \Delta t}{N_2} i\right), \end{cases} \tag{4.4}$$

where $k = \mathbb{Q}(a, b, c, d, \Delta t, N_1, N_2)$ with σ acting as the identity on k.

- To verify whether I, i can be eliminated from (4.4), we consider the affine variety defined by (4.4) over $\mathbb{Q}(a, b, c, d, \Delta t, N_1, N_2, s, \sigma(s), S, \sigma(S))$, and so $d = 0, D = 1$, thus
$$B(d, D) - 1 = 2 - 1 = 1.$$

- To verify whether I, i, s can be eliminated from (4.4), we consider the affine variety defined by (4.4) over $\mathbb{Q}(a, b, c, d, \Delta t, N_1, N_2, S, \sigma(S))$, and so $d = 2, D = 2$. We compute
$$B(2, 2) - 1 = 135 - 1 = 134.$$

It turns out to be computationally feasible to carry out a computation with 134 transforms and probability $p = 0.99$ as described in Remark 4.2. The output of the computation is that the elimination is possible.

Example 4.8. Let F_n be the n-th Fibonacci number. It turns out [10, p. 856] that the sequence $A_n := F_{2^n}$ satisfies a nonlinear difference equation. Such an equation can be found using difference elimination as follows. We introduce $B_n := F_{2^n+1}$. Then standard identities $F_{2k} = F_k(2F_{k+1} - F_k)$ and $F_{2k+1} = F_{k+1}^2 + F_k^2$ for the Fibonacci numbers imply the following system of difference equations

$$\begin{cases} A_{n+1} = A_n(2B_n - A_n), \\ B_{n+1} = A_n^2 + B_n^2. \end{cases} \tag{4.5}$$

Considered as a system of polynomial equations in B_n and B_{n+1}, (4.5) defines an affine variety of dimension zero and degree two over $\mathbb{Q}(A_n, A_{n+1})$. Theorem 3.4 implies that it is sufficient to consider system (4.5) and two of its transforms to eliminate B. Performing this elimination, we find the difference equation

$$5F_{2^n}^4 F_{2^{n+1}} - 2F_{2^n}^2 F_{2^{n+2}} + F_{2^{n+1}}^3 = 0,$$

giving an alternative to the difference equation stated in [10, p. 856]. Our approach to finding a difference equation for F_{2^n} can be viewed as a generalization of the transfer matrix method [34, §4.7] to the case of nonlinear recurrences.

Example 4.9. The following example shows that our bound is sharp in the case $d = 0$ (this is the case in Examples 4.4, 4.6, and 4.8). We fix a positive integer D and consider the system

$$\begin{cases} x(x - 1) \cdot \ldots \cdot (x - D + 1) = 0, \\ \sigma(x) - x - 1 = 0. \end{cases} \tag{4.6}$$

System (4.6) does not have a solution in $\mathbb{C}^\mathbb{Z}$, because the elements of the solution can only take values from $0, 1, \ldots, D - 1$ and strictly increase. On the other hand, the system

consisting of the 0-th,... , $D - 1 = (B(0, D) - 2)$-th transforms of (4.6) has a solution $\sigma^i(x) = i$ for $0 \leqslant i \leqslant D$. Hence, it is necessary to consider one more transform in order to express 1 (i.e. eliminate x).

Example 4.10. This example obtained by analyzing the proof of Proposition 6.24 shows that our bound is sharp for $d = 1$ and $D = 2$. Consider a system of difference equations given by any set of generators of the polynomial ideal $I := I_1 \cap I_2$ of the polynomial ring $\mathbb{Q}[x, \sigma(x), y, \sigma(y)]$, where

$$I_1 := \langle x, \sigma(x) + \sigma(y) - 1, y + 2\sigma(y) - 1 \rangle, \quad I_2 := \langle \sigma(x), y, x + 3\sigma(y) - 1 \rangle.$$

The variety X defined by I is a union of two affine subspaces of dimension one, so $d = \dim X = 1$ and $D = \deg X = 2$. Thus, $B(d, D) - 1 = 6$. Our computation in MAPLE shows that

$$1 \in \langle I, \sigma(I), \ldots, \sigma^6(I) \rangle \quad \text{but} \quad 1 \notin \langle I, \sigma(I), \ldots, \sigma^5(I) \rangle.$$

Thus, our bound for $d = 1$ and $D = 2$ is sharp.

5 Counterexamples

5.1 Failure of the standard DEP method

Consider the system of difference equations given by any set of generators of the polynomial ideal $I := I_1 \cap I_2$ of the polynomial ring $\mathbb{Q}[x, \sigma(x), y, \sigma(y), z, w]$, where

$$I_1 := \langle \sigma(y)z - 1, x, \sigma(x) - y \rangle, \quad I_2 := \langle \sigma(x), \sigma(y) - 1, (y - 1)z - 1, (x - 1)w - 1 \rangle.$$

We do not present the actual generators of I due to the size of this set, the generators can be computed by a computer algebra system such as MAPLE. A computation in MAPLE shows that

$$1 \in \langle I, \sigma(I), \sigma^2(I), \sigma^3(I), \sigma^4(I) \rangle.$$

Therefore, by Proposition 6.3, the system has no solutions in any difference ring. Using MAPLE, one can also verify that

$$I = \langle I, \sigma(I) \rangle \cap \mathbb{Q}[x, \sigma(x), y, \sigma(y), z, w], \tag{5.1}$$
$$\sigma(I) = \langle I, \sigma(I) \rangle \cap \mathbb{Q}[\sigma(x), \sigma^2(x), \sigma(y), \sigma^2(y), \sigma(z), \sigma(w)]. \tag{5.2}$$

Most of the existing effective bounds for systems of ordinary differential and difference equations [3, 9, 19, 20, 29] use sufficient conditions for the existence of a solution based on the system and its first prolongation (differential equations) or first transform (difference equations), introduced for difference equations in [6, Section 14, Chapter 8] and

also known as geometric axioms [5, 30] in model theory, which are summarized under the DEP method mentioned in the introduction. In our case, it is tempting to formulate an analogue of such conditions as:

> Let Γ be the affine variety defined by the system and its first transform. If the projections of Γ onto the varieties defined by the system and by its first transform alone, respectively, are dominant, then the system is consistent.

However, this is false in the above example as we have shown, where Γ is the affine variety corresponding to the ideal $\langle I, \sigma(I) \rangle$ in the affine space with coordinates $x, \sigma(x), \sigma^2(x), y, \sigma(y), \sigma^2(y), z, \sigma(z), w, \sigma(w)$, and (the Zariski closures of) the projections are given by the intersections in (5.1) and (5.2).

5.2 Non-existence of coefficient-independent effective strong Nullstellensatz

A (non-effective) strong Nullstellensatz for systems of difference equations can be stated as follows. Let $f_1 = \ldots = f_N = 0$ be a system of difference equations. If a difference polynomial f vanishes at all solutions of the system in $\mathbb{C}^{\mathbb{N}}$, then there exists ℓ such that f belongs to the radical of the ideal generated by the 0-th,..., ℓ-th transforms of $f_1, \ldots, f_N$.

The following example shows that there is no uniform upper bound for this ℓ in terms of the degree, order, and number of variables of $f_1, \ldots, f_N$. For every positive integer M, consider

$$\begin{cases} f_1 = \sigma(x) - x - \frac{1}{M} = 0, \\ f_2 = x\,(y(x-1) - 1) = 0. \end{cases} \tag{5.3}$$

Let $f = y(x-1) - 1$ and $x = \{x_n\}_{n=0}^{\infty}$ and $y = \{y_n\}_{n=0}^{\infty}$ any solution of (5.3) in $\mathbb{C}^{\mathbb{N}}$. If $y_k(x_k - 1) - 1 \neq 0$ for some k, then $x_k = 0$. Hence, $x_{k+M} = 1$, and so

$$x_{k+M}\,(y_{k+M}(x_{k+M} - 1) - 1) = -1.$$

Therefore, f vanishes at every solution of (5.3) in $\mathbb{C}^{\mathbb{N}}$. However, f does not belong to the radical of the ideal generated by the 0-th,..., $(M-1)$-th transforms of f_1 and f_2. These transforms belong to the polynomial ring $\mathbb{C}[x, \ldots, \sigma^M(x), y, \ldots, \sigma^{M-1}(y)]$. Consider the substitution

$$\sigma^k(x) = \frac{k}{M} \text{ for every } 0 \leqslant k \leqslant M, \quad \sigma^k(y) = \frac{M}{k - M} \text{ for every } 1 \leqslant k \leqslant M - 1, \quad y = 0.$$

A direct computation shows that the polynomials $f_1, \ldots, \sigma^{M-1}(f_1), f_2, \ldots, \sigma^{M-1}(f_2)$ vanish after this substitution, but f does not.

5.3 Non-existence of coefficient-independent effective full elimination theorem.

Let $F \subset k\{\mathbf{x}, \mathbf{u}\}$ be a finite set of difference polynomials and h a positive integer. Since $k[\mathbf{x}, \ldots, \sigma^h(\mathbf{x})]$ is Noetherian, there exists a positive integer ℓ such that

$$\langle \sigma^i(F) \mid 0 \leqslant i < \infty \rangle \cap k[\mathbf{x}, \ldots, \sigma^h(\mathbf{x})] = \langle \sigma^i(F) \mid 0 \leqslant i < \ell \rangle \cap k[\mathbf{x}, \ldots, \sigma^h(\mathbf{x})]. \tag{5.4}$$

A bound on such an ℓ in terms of h, degrees and orders of F, and the number of variables would be a natural difference counterpart of the full elimination result for differential-algebraic equations [29, Theorem 3]. However, the following modification of the example from Section 5.2 shows that such a bound does not exist. We fix a positive integer M and consider system (5.3) with one extra equation

$$f_3 = z - y(x - 1) + 1 = 0,$$

where z is a new unknown. We have shown in Section 5.2 that $y(x - 1) - 1$ vanishes on every solution of (5.3) in $\mathbb{C}^{\mathbb{N}}$. Then z vanishes on every solution of $f_1 = f_2 = f_3 = 0$ in $\mathbb{C}^{\mathbb{N}}$. Then Hilbert's Nullstellensatz [33, Tag 00FU] combined with the Rabinowitz trick implies that there exists a positive integer N such that

$$z^N \in \langle \sigma^i(\{f_1, f_2, f_3\}) \mid 0 \leqslant i < \infty \rangle.$$

On the other hand, following the argument from Section 5.2, we see that

$$z^N \notin \langle \sigma^i(\{f_1, f_2, f_3\}) \mid 0 \leqslant i < M \rangle.$$

Thus, an integer ℓ such that

$$\langle \sigma^i(\{f_1, f_2, f_3\}) \mid 0 \leqslant i < \infty \rangle \cap \mathbb{C}[z] = \langle \sigma^i(\{f_1, f_2, f_3\}) \mid 0 \leqslant i < \ell \rangle \cap \mathbb{C}[z]$$

must satisfy $\ell \geqslant M$. Hence there is no coefficient-independent bound for such an ℓ.

6 Proofs of the main results

6.1 Difference Nullstellensatz

Definition 6.1 (Inversive difference rings)**.**

- We say that a difference ring (A, σ) is *inversive* if $\sigma : A \to A$ is an automorphism.

- For any difference ring (A, σ), there is an inversive difference ring $(A^{\mathrm{inv}}, \sigma)$ and a map of difference ring $(A, \sigma) \to (A^{\mathrm{inv}}, \sigma)$ that is universal for maps from (A, σ) to inversive difference rings (see [25, Proposition 2.1.7]).

- Given a difference ring (A, σ), the *ring of inversive difference polynomials* over A in the variables, $A\{x_1, \ldots, x_n\}^*$, is realized as the ordinary polynomial ring over A in the formal variables $\sigma^j(x_i)$, for $j \in \mathbb{Z}$ and $1 \le i \le n$, with σ extending the given endomorphism on A and

$$\sigma(\sigma^j(x_i)) = \sigma^{j+1}(x_i)$$

  on the variables.

- If (A, σ) is inversive, then so is $A\{x_1, \ldots, x_n\}^*$.

Definition 6.2. Let k be a difference field, $F \subset k\{x_1, \ldots, x_n\}$ a finite set of difference polynomials, and $h = \max\{\operatorname{ord} f \mid f \in F\}$. The set of n tuples $\mathbf{a}_1, \ldots, \mathbf{a}_n \in k^{\ell+h}$, where $\mathbf{a}_i := (a_{i,0}, \ldots, a_{i,\ell+h-1})$, is called *a partial solution of length ℓ* if, for every $f \in F$ and $0 \le s \le \ell - 1$, the polynomial $\sigma^s(f)$ vanishes after the substitution

$$\sigma^i(x_j) = a_{j,i} \text{ for every } 1 \le j \le n, \quad 0 \le i \le \ell + h - 1.$$

Let K be an inversive difference field. Then the difference ring of sequences $K^{\mathbb{Z}}$ with respect to the shift automorphism can be endowed with a structure of a difference K-algebra via the embedding of difference rings $i_K \colon K \to K^{\mathbb{Z}}$ defined by

$$i_K(f) = \left(\ldots, \sigma^{-1}(f), f, \sigma(f), \sigma^2(f), \ldots\right) \text{ for } f \in K.$$

This can be similarly done for $K^{\mathbb{N}}$.

Proposition 6.3. *For all uncountable algebraically closed inversive difference fields K and finite sets $F \subseteq K\{x_1, \ldots, x_n\}$, the following statements are equivalent:*

1. *F has a solution in $K^{\mathbb{Z}}$.*

2. *F has a solution in $K^{\mathbb{N}}$.*

3. *F has finite partial solutions of length ℓ for all $\ell \gg 0$.*

4. *The ideal $[F] := \langle \{\sigma^j(F) \mid j \in \mathbb{N}\} \rangle \subseteq K\{x_1, \ldots, x_n\}$ does not contain 1.*

5. *The ideal $[F]^* := \langle \{\sigma^j(F) \mid j \in \mathbb{Z}\} \rangle \subseteq K\{x_1, \ldots, x_n\}^*$ does not contain 1.*

6. *F has a solution in some difference K-algebra.*

Proof. The implications $1 \implies 2$, $2 \implies 3$, and $6 \implies 4$ are straightforward.

$3 \implies 4$. Assume that there exist arbitrarily long partial solutions, but $1 \in [F]$. Then there is an expression of the form

$$1 = \sum_{i=0}^{\ell} \sum_{f \in F} a_{i,f} \sigma^i(f), \tag{6.1}$$

where $a_{i,f} \in K\{x_1, \ldots, x_n\}$. Let $h = \max\{\operatorname{ord} f \mid f \in F\}$. Consider a partial solution of F of length $\ell + h + 1$ and plug it into the equality (6.1). Then the right-hand side will vanish, so we arrive at contradiction.

$4 \implies 5$. Assume that $1 \in [F]^*$. We fix some representation of 1 as an element of $[F]^*$. Let N be the maximum number such that $\sigma^{-N}(x_i)$ occurs in the representation. Applying σ^N to both sides of the representation, we obtain a representation of 1 as an element of $[F]$.

$5 \implies 6$. Let $\pi \colon K\{x_1, \ldots, x_n\}^* \to K\{x_1, \ldots, x_n\}^*/[F]^*$ be the canonical surjection. Then $(\pi(x_1), \ldots, \pi(x_n))$ is a solution of F in $K\{x_1, \ldots, x_n\}^*/[F]^*$.

$5 \implies 1$. Let E be the inversive difference subfield of K generated by the coefficients of elements of F over the prime subfield of K. Since 1 does not belong to $[F]^* \cap E\{x_1, \ldots, x_n\}^*$, there exists a maximal (not necessarily difference) ideal $\mathfrak{m} \subset E\{x_1, \ldots, x_n\}^*$ containing $[F]^* \cap E\{x_1, \ldots, x_n\}^*$. Then $L := E\{x_1, \ldots, x_n\}^*/\mathfrak{m}$ is a field, and the transcendence degree of L over E is at most countable. Since K is algebraically closed and has uncountable transcendence degree, there exists an embedding $\varphi \colon L \to K$ over the common subfield E. Composing φ with the canonical surjection $E\{x_1, \ldots, x_n\}^* \to L$, we obtain an E-algebra homomorphism $\psi \colon E\{x_1, \ldots, x_n\}^* \to K$ such that $[F]^* \subset \operatorname{Ker} \psi$. For every $1 \leqslant i \leqslant n$, we construct a sequence $\mathbf{a}_i := \{a_{i,j}\}_{j \in \mathbb{Z}} \in K^{\mathbb{Z}}$ by the formula

$$a_{i,j} = \psi\left(\sigma^j(x_i)\right).$$

A direct computation shows that $(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ is a solution of F in $K^{\mathbb{Z}}$. $\qquad \square$

6.2 Variety and two projections

Let k be a difference field and $F = 0$ a system of difference equations, where $F = \{f_1, \ldots, f_N\} \subset k\{u_1, \ldots, u_r\}$. We set

$$h_i := \max_{j=1,\ldots,N} \operatorname{ord}_{u_i} f_j \quad \text{and} \quad H = h_1 + \ldots + h_r + r.$$

For the rest of Section 6, we fix K to be an inversive uncountable algebraically closed difference field containing k. With the system $F = 0$ of difference equations, we associate the following geometric data:

- the subvariety X of $\mathbb{A}^H$ defined by the polynomials $f_1, \ldots, f_N$;

- two projections $\pi_1, \pi_2 \colon \mathbb{A}^H \to \mathbb{A}^{H-r}$ defined by

$$\pi_1\left(u_1, \ldots, \sigma^{h_1}(u_1), u_2, \ldots, \sigma^{h_r}(u_r)\right) := \left(u_1, \ldots, \sigma^{h_1-1}(u_1), u_2, \ldots, \sigma^{h_r-1}(u_r)\right),$$
(6.2)

$$\pi_2\left(u_1, \ldots, \sigma^{h_1}(u_1), u_2, \ldots, \sigma^{h_r}(u_r)\right) := \left(\sigma(u_1), \ldots, \sigma^{h_1}(u_1), \sigma(u_2), \ldots, \sigma^{h_r}(u_r)\right).$$
(6.3)

Let $Z \subset \mathbb{A}^H$ be a variety defined by polynomials $g_1, \ldots, g_s \in K[\mathbb{A}^H]$. Let $\sigma^i(Z)$, where $i \in \mathbb{Z}$, denote the variety defined by the polynomials $g_1^{\sigma^i}, \ldots, g_s^{\sigma^i} \in K[\mathbb{A}^H]$, where g^{σ^i} means the result of applying σ^i to all coefficients of g. The coordinate-wise application of σ^i defines a bijection between Z and $\sigma^i(Z)$.

Definition 6.4. A sequence $p_1, \ldots, p_\ell \in \mathbb{A}^H(K)$ is *a partial solution* of the triple (X, π_1, π_2) if

$$\begin{cases} \pi_1(p_{i+1}) = \pi_2(p_i) \text{ for every } 1 \leqslant i < \ell, \\ p_i \in \sigma^{i-1}(X)(K) \text{ for every } 1 \leqslant i \leqslant \ell. \end{cases}$$

A two-sided infinite sequence with such a property is called *a solution* of the triple (X, π_1, π_2).

Lemma 6.5. *For every positive integer ℓ, the system $F = 0$ has a partial solution of length ℓ if and only if the triple (X, π_1, π_2) has a partial solution of length ℓ.*

The system $F = 0$ has a solution in $K^{\mathbb{Z}}$ if and only if the triple (X, π_1, π_2) has an infinite solution.

Proof. Let $h = \max\limits_{1 \leqslant i \leqslant r} h_i$. Consider a partial solution $\mathbf{u}_1, \ldots, \mathbf{u}_r \in K^{\ell+h}$ of F, where $\mathbf{u}_i = (u_{i,1}, \ldots, u_{i,\ell+h})$ for every $1 \leqslant i \leqslant r$. We set

$$p_j := (u_{1,j}, \ldots, u_{1,j+h_1}, u_{2,j}, \ldots, u_{r,j+h_r}) \text{ for every } 1 \leqslant j \leqslant \ell.$$

By the construction

$$\pi_2(p_j) = (u_{1,j+1}, \ldots, u_{1,j+h_1}, u_{2,j+1}, \ldots, u_{r,j+h_r}) = \pi_1(p_{j+1}),$$

so $p_{j+1} \in \pi_1^{-1}(\pi_2(p_j))$ for every $1 \leqslant j \leqslant \ell - 1$. The definition of partial solution implies that $p_j \in \sigma^{j-1}(X)$ for every $1 \leqslant j \leqslant \ell$. Hence, $p_1, \ldots, p_\ell$ is a partial solution of the triple (X, π_1, π_2). The above argument can be straightforwardly reversed to construct a partial solution of F from a partial solution of (X, π_1, π_2). The case of infinite solutions is completely analogous. $\qquad\square$

In the introduced geometric language, we can formulate the following question equivalent to an effective difference Nullstellensatz

Question 6.6. *Let X be an algebraic subvariety of $\mathbb{A}^H$ and π_1, π_2 be the surjective linear maps $\mathbb{A}^H \to \mathbb{A}^{H-r}$ defined by (6.2) and (6.3). How long a partial solution of (X, π_1, π_2) is it sufficient to find in order to conclude that the triple (X, π_1, π_2) has an infinite solution?*

Thus, in what follows, we fix a triple (X, π_1, π_2), where X is an algebraic subvariety of $\mathbb{A}^H$ and π_1, π_2 are surjective linear maps $\mathbb{A}^H \to \mathbb{A}^{H-r}$ defined over the σ-constants of K.

6.2.1 Trains

The goal of this section is to generalize the notion of a solution of the triple to not necessarily zero-dimensional points.

Definition 6.7. For ℓ a positive integer or $+\infty$, a sequence of irreducible subvarieties $(Y_1, \ldots, Y_\ell)$ in $\mathbb{A}^H$ is said to be *a train* of length ℓ in X if

$$\begin{cases} \overline{\pi_1(Y_{i+1})} = \overline{\pi_2(Y_i)} \text{ for every } 1 \leqslant i < \ell, \text{ where } \overline{Y} \text{ denotes the Zariski closure of } Y, \\ Y_i \subset \sigma^{i-1}(X) \text{ for every } 1 \leqslant i \leqslant \ell. \end{cases}$$

Remark 6.8. Let $p_1, \ldots, p_\ell \in \mathbb{A}^H$ be a partial solution of (X, π_1, π_2) (see Definition 6.4). Considering the singletons $\{p_1\}, \ldots, \{p_\ell\}$ as irreducible zero-dimensional subvarieties of $\mathbb{A}^H$, we see that $(\{p_1\}, \ldots, \{p_\ell\})$ is a train in X.

Lemma 6.9. *For every train $(Y_1, \ldots, Y_\ell)$ in X, there exists a partial solution $p_1, \ldots, p_\ell$ of (X, π_1, π_2) such that, for all i, $1 \leqslant i \leqslant \ell$, we have $p_i \in Y_i$.*

Proof. We will prove the following statement by induction on ℓ: there exists a nonempty open subset $U \subset Y_\ell$ such that, for every point $p_\ell \in U$, there exists a partial solution $p_1, \ldots, p_\ell$ of (X, π_1, π_2) such that, for every i, $1 \leqslant i \leqslant \ell$, we have $p_i \in Y_i$. In the case $\ell = 1$, we can set $U = Y_1$, because every single point in X is a partial solution of length one.

Assume that $\ell > 1$. Applying the inductive hypothesis to the train $(Y_1, \ldots, Y_{\ell-1})$, we obtain an open nonempty subset $U_0 \subset Y_{\ell-1}$. Since U_0 is dense in $Y_{\ell-1}$, $\pi_2(U_0)$ is dense in $\overline{\pi_2(Y_{\ell-1})} = \overline{\pi_1(Y_\ell)}$. Since $\pi_1(Y_\ell)$ is a constructible dense subset in $\overline{\pi_1(Y_\ell)}$, $\pi_2(U_0) \cap \pi_1(Y_\ell)$ is also dense constructible in $\overline{\pi_1(Y_\ell)}$. Let $U_1 \subset \pi_2(U_0) \cap \pi_1(Y_\ell)$ be an open dense subset of $\overline{\pi_1(Y_\ell)}$. Then $U_2 := Y_\ell \cap \pi_1^{-1}(U_1)$ is nonempty open in Y_ℓ. We claim that every point $p_\ell \in U_2$ can be extended to a partial solution $p_1, \ldots, p_\ell$ such that $p_i \in Y_i$. By the definition of U_2, $\pi_1(p_\ell) \in \pi_2(U_0)$, so there exists $p_{\ell-1} \in U_0$ such that $\pi_2(p_{\ell-1}) = \pi_1(p_\ell)$. By the inductive hypothesis, $p_{\ell-1}$ can be further extended to a partial solution. $\qquad\square$

Corollary 6.10. *If there is an infinite train in X, then there is a solution for the triple (X, π_1, π_2).*

Proof. Since there is an infinite train, there are arbitrarily long finite trains. Due to Lemma 6.9, there are arbitrarily long finite partial solutions of (X, π_1, π_2). Lemma 6.5 implies that there are arbitrarily long finite partial solutions of the corresponding system F. Hence, due to Proposition 6.3, there is a solution of F in $K^{\mathbb{Z}}$. Lemma 6.5 implies that there exists an infinite solution of the triple (X, π_1, π_2). $\qquad\square$

Definition 6.11 (Train operations)**.**

- For two trains Y and Y' of the same length, the inclusion $Y \subset Y'$ is understood as a component-wise containment.

- For a train Y in X and $i \in \mathbb{Z}$, $\sigma^i(Y)$ is the result of the component-wise application of σ^i to Y, and, since π_1 and π_2 are defined over the constants, $\sigma^i(Y)$ is a train in $\sigma^i(X)$.

Remark 6.12. Since the component-wise union of any chain of trains of the same length is again a train of this length, trains of fixed length satisfy Zorn's lemma with respect to inclusion. Hence, maximal trains of a fixed length are well-defined.

6.2.2 The number of maximal trains

Our next Lemma 6.13 appears to be part of the folklore, but for want of a written reference, we offer a proof here.

Lemma 6.13. *Let $\varphi_X \colon X \to Z$ and $\varphi_Y \colon Y \to Z$ be dominant morphisms of affine varieties over an algebraically closed field. Assume that X and Y are irreducible. Consider the fibered product $X \times_Z Y$ of φ_X and φ_Y, considered as a variety, and denote the natural morphisms to X and Y by π_X and π_Y, respectively. Then there exists an irreducible component $V \subset X \times_Z Y$ such that the restrictions of both π_X and π_Y to V are dominant.*

Proof. Denote the algebras of regular functions on X, Y, and Z by A, B, and C, respectively. Since X, Y, and Z are irreducible (Z is irreducible as an image of an irreducible variety under a dominant morphism), these algebras are domains. We denote the fields of fractions of A, B, and C by E, F, and L, respectively. The dominant maps φ_X and φ_Y give rise to injective homomorphisms $\varphi_X^\# \colon C \to A$ and $\varphi_Y^\# \colon C \to B$. These homomorphisms equip A and B with a C-algebra structure. Then, the algebra of regular functions on $X \times_Z Y$, as a scheme, is $A \otimes_C B$ (see [33, Tag 01I4]).

Let $\mathfrak{p}$ be any prime ideal in $E \otimes_L F$. Let $D := (E \otimes_L F)/\mathfrak{p}$ and $\pi \colon E \otimes_L F \to D$ be the canonical projection. Consider the natural homomorphism $i \colon A \otimes_C B \to E \otimes_L F$. Since $1 \in i(A \otimes_C B)$, the composition $\pi \circ i$ is a nonzero homomorphism. Consider the natural embeddings $i_A \colon A \to A \otimes_C B$ and $i_B \colon B \to A \otimes_C B$. We will show that the compositions $\pi \circ i \circ i_A \colon A \to D$ and $\pi \circ i \circ i_B \colon B \to D$ are injective. Introducing the natural embeddings $i_E \colon E \to E \otimes_L F$ and $j_A \colon A \to E$, we can rewrite

$$\pi \circ i \circ i_A = \pi \circ i_E \circ j_A.$$

The homomorphisms i_E and j_A are injective. The restriction of π to $i_E(E)$ is also injective, since E is a field. Hence, the whole composition $\pi \circ i_E \circ j_A$ is injective. The argument for $\pi \circ i \circ i_B$ is analogous.

Thus, we have an irreducible subvariety of $X \times_Z Y$, and hence of the variety $(X \times_Z Y)_{\mathrm{red}}$ [33, Tag 0356], defined by the ideal $\mathrm{Ker}(\pi \circ i)$ that projects dominantly on both X and Y. Hence, the component containing this subvariety also projects dominantly on X and Y. □

Definition 6.14 (Marked trains). Let $X_1 \cup X_2 \cup \ldots \cup X_s$ be the decomposition of X into irreducible components.

- A pair $(Y, \mathbf{c})$, where $Y = (Y_1, \ldots, Y_\ell)$ is a train in X and $\mathbf{c} = (c_1, \ldots, c_\ell) \in \{1, \ldots, s\}^\ell$, is called a *marked train* of length ℓ and *signature* $\mathbf{c}$ if $Y_i \subset \sigma^{i-1}(X_{c_i})$ for every $1 \leqslant i \leqslant \ell$.

- Every train has at least one signature (maybe several), so that it becomes a marked train.

- Analogously to trains, we define a notion of a maximal train of given length ℓ and signature $\mathbf{c}$.

Let $\mathbf{c} = (c_1, \ldots, c_\ell) \in \{1, \ldots, s\}^\ell$ be a tuple. Consider

$$X^{\mathbf{c}} := X_{c_1} \times \sigma(X_{c_2}) \times \ldots \times \sigma^{\ell-1}(X_{c_\ell}) \subset (\mathbb{A}^H)^\ell.$$

We denote the projections $(\mathbb{A}^H)^\ell \to \mathbb{A}^H$ onto the components by $\psi_{\ell,1}, \ldots, \psi_{\ell,\ell}$, respectively. We introduce

$$W_{\mathbf{c}} := \left\{ p \in X^{\mathbf{c}} \mid \pi_2\left(\psi_{\ell,i}(p)\right) = \pi_1\left(\psi_{\ell,i+1}(p)\right) \text{ for all } i, \ 1 \leqslant i < \ell \right\}. \tag{6.4}$$

The restrictions of $\psi_{\ell,1}, \ldots, \psi_{\ell,\ell}$ to $W_{\mathbf{c}}$ will be denoted by the same symbols.

Lemma 6.15. *For every irreducible subvariety $Z \subset W_{\mathbf{c}}$,*

$$\left(\overline{\psi_{\ell,1}(Z)}, \ldots, \overline{\psi_{\ell,\ell}(Z)} \right)$$

is a marked train of signature $\mathbf{c}$.

Proof. For every i, $1 \leqslant i \leqslant \ell$,

$$Y_i := \overline{\psi_{\ell,i}(Z)} \subset \overline{\psi_{\ell,i}(W_{\mathbf{c}})} \subset \sigma^{i-1}(X_{c_i}).$$

Moreover, since Z is irreducible, $\overline{\psi_{\ell,i}(Z)}$ is also irreducible. Fix some i, $1 \leqslant i < \ell$. We will show that $\overline{\pi_2(Y_i)} = \overline{\pi_1(Y_{i+1})}$. We can write $\overline{\pi_2(Y_i)}$ as $\overline{\pi_2(\psi_{\ell,i}(Z))}$. By (6.4), the latter is equal to $\overline{\pi_1(\psi_{\ell,i+1}(Z))}$, which is the same as $\overline{\pi_1(Y_{i+1})}$. □

Lemma 6.16. *For every marked train $(Y_1, \ldots, Y_\ell)$ of signature $\mathbf{c}$ in X, there exists an irreducible subvariety $Y \subset W_{\mathbf{c}}$ such that, for every i, $1 \leqslant i \leqslant \ell$, we have $Y_i = \overline{\psi_{\ell,i}(Y)}$.*

Proof. We will prove the lemma by induction on ℓ. For $\ell = 1$, $\mathbf{c} = (c_1)$, $W_{\mathbf{c}} = X_{c_1}$, and we can set $Y = Y_1$.

Let $\ell > 1$. Apply the inductive hypothesis to the train $(Y_1, \ldots, Y_{\ell-1})$ of signature $\mathbf{c}' := (c_1, \ldots, c_{\ell-1})$ and obtain an irreducible subvariety $Y' \subset W_{\mathbf{c}'} \subset (\mathbb{A}^H)^{\ell-1}$. Then there is a natural embedding of $Y' \times Y_\ell$ into $(\mathbb{A}^H)^\ell$. Denote $(Y' \times Y_\ell) \cap W_{\mathbf{c}}$ by W. Since Y' is already contained in $W_{\mathbf{c}'}$,

$$W = \{p \in Y' \times Y_\ell \mid \pi_2\left(\psi_{\ell,\ell-1}(p)\right) = \pi_1\left(\psi_{\ell,\ell}(p)\right)\}. \tag{6.5}$$

Let $\psi = (\psi_{\ell,1}, \psi_{\ell,2}, \ldots, \psi_{\ell,\ell-1}) \colon (\mathbb{A}^H)^\ell \to (\mathbb{A}^H)^{\ell-1}$ and

$$Z := \overline{\pi_2\left(\psi_{\ell-1,\ell-1}(Y')\right)} = \overline{\pi_1(Y_\ell)}. \tag{6.6}$$

Then equality (6.5) implies (see [15, Ex. 2.26]) that W together with the morphisms $\psi \colon W \to Y'$ and $\psi_{\ell,\ell} \colon W \to Y_\ell$ is the fibered product of the morphisms $\pi_2 \circ \psi_{\ell-1,\ell-1} \colon Y' \to Z$ and $\pi_1 \colon Y_\ell \to Z$. Equality (6.6) implies that both of these morphisms are dominant.

Due to Lemma 6.13, there exists an irreducible subset $Y \subset W$ such that $\psi \colon Y \to Y'$ and $\psi_{\ell,\ell} \colon Y \to Y_\ell$ are dominant. For every i, $1 \leqslant i < \ell$, since $\psi_{\ell,i} = \psi_{\ell-1,i} \circ \psi$, the restriction $\psi_{\ell,i} \colon Y \to Y_i$ is dominant as a composition of two dominant morphisms. $\qquad\square$

Lemma 6.17. *Let the degree of X_i be D_i (see Definition 2.10), and fix a tuple $\mathbf{c} = (c_1, \ldots, c_\ell) \in \{1, \ldots, s\}^\ell$. The number of maximal trains of signature $\mathbf{c}$ in X does not exceed $D_{c_1} \cdot D_{c_2} \cdot \ldots \cdot D_{c_\ell}$.*

Proof. Since $W_{\mathbf{c}}$ is the intersection of $X^{\mathbf{c}}$ with a linear subspace,

$$\deg W_{\mathbf{c}} \leqslant \deg X^{\mathbf{c}} = \deg X_{c_1} \cdot \deg \sigma(X_{c_2}) \cdot \ldots \cdot \deg \sigma^{\ell-1}(X_{c_\ell}). \tag{6.7}$$

Since application of σ to a variety does not change the degree, the product in (6.7) does not exceed $D_{c_1} \cdot \ldots \cdot D_{c_\ell}$. Hence, the number of components of $W_{\mathbf{c}}$ does not exceed $D_{c_1} \cdot \ldots \cdot D_{c_\ell}$.

Let $(Y_1, \ldots, Y_\ell)$ be a maximal train in X of signature $\mathbf{c}$. Lemma 6.16 implies that there exists an irreducible subvariety $Y \subset W_{\mathbf{c}}$ such that for every i, $1 \leqslant i \leqslant \ell$, we have $Y_i = \overline{\psi_{\ell,i}(Y)}$. Let C be an irreducible component of $W_{\mathbf{c}}$ containing Y. Lemma 6.15 implies that

$$\left(\overline{\psi_{\ell,1}(C)}, \ldots, \overline{\psi_{\ell,\ell}(C)}\right)$$

is also a train of signature $\mathbf{c}$. Moreover, since $C \supset Y$, this train contains $(Y_1, \ldots, Y_\ell)$. The maximality of the latter implies that these trains are equal. Hence, Y could be chosen to be an irreducible component of $W_{\mathbf{c}}$. Thus, we obtain an injective map from the set of maximal trains of signature $\mathbf{c}$ to the set of all irreducible component of $W_{\mathbf{c}}$. Hence, the number of maximal trains also does not exceed $D_{c_1} \cdot \ldots \cdot D_{c_\ell}$. $\qquad\square$

Corollary 6.18. *The number of maximal trains in X of length ℓ does not exceed $(\deg X)^{\ell}$.*

Proof. Since every maximal train can be considered as a marked maximal train, the number of maximal trains of length ℓ in X does not exceed the sum of products $D_{c_1} \cdot \ldots \cdot D_{c_{\ell}}$ over all tuples $\mathbf{c}$ of length ℓ. This sum is equal to

$$\sum_{c_1=1}^{s} \sum_{c_2=1}^{s} \cdots \sum_{c_{\ell}=1}^{s} \prod_{i=1}^{\ell} D_{c_i} = (D_1 + \ldots + D_s)^{\ell} = D^{\ell}. \qquad \square$$

6.2.3 A bound for trains

Definition 6.19. For a train $Y = (Y_1, \ldots, Y_{\ell})$ in X, we introduce the codimension of Y as

$$\operatorname{codim} Y := \dim X - \min_{1 \leqslant i \leqslant \ell} \dim Y_i.$$

Definition 6.20. We call a train $Y = (Y_1, \ldots, Y_{\ell})$ in X *skew-cyclic* if $\ell > 1$ and $Y_{\ell} = \sigma^{\ell-1}(Y_1)$.

Lemma 6.21. *If there exists a skew-cyclic train in X of codimension d, then there exists an infinite train in X of codimension d.*

Proof. Let $(Y_1, \ldots, Y_{\ell})$ be a skew-cyclic train in X of codimension d. Then we can construct an infinite train of codimension d as follows:

$$\left(Y_1, Y_2, \ldots, Y_{\ell-1}, \sigma^{\ell-1}(Y_1), \sigma^{\ell-1}(Y_2), \ldots, \sigma^{\ell-1}(Y_{\ell-1}), \sigma^{2\ell-1}(Y_1), \ldots \right). \qquad \square$$

Definition 6.22. We define $B'(d, D)$ to be the smallest natural number N such that, for every triple (X, π_1, π_2) such that the $\deg X \leqslant D$, the existence of a train of length N and codimension at most d in X implies the existence of a skew-cyclic train in X of length at most N and codimension at most d, or ∞ if such N does not exist.

The following statement implies that $B'(d, D)$ is finite for all $d \in \mathbb{Z}_{\geqslant 0}$ and $D \in \mathbb{Z}_{>0}$ and gives an upper bound for $B'(d, D)$.

Proposition 6.23. *For all $D \in \mathbb{Z}_{>0}$,*

1. *$B'(0, D) \leqslant D + 1$ and*

2. *for every $d \in \mathbb{Z}_{\geqslant 0}$, $B'(d+1, D) \leqslant B'(d, D) + D^{B'(d,D)}$.*

Proof. Throughout the proof, we will use the observation that the existence of a skew-cyclic train in $\sigma^i(X)$ for some $i \in \mathbb{Z}$ implies (via component-wise application of σ^{-i}) the existence of a skew-cyclic train of the same codimension in X.

We prove the first statement of the proposition. Consider a train $(Y_1, \ldots, Y_{D+1})$ of codimension zero and length $D + 1$. Since, for every i, $1 \leqslant i \leqslant D + 1$, we have $\dim Y_i = \dim X$, then every $\sigma^{-i+1}(Y_i)$ is an irreducible component of X. The number of components of X does not exceed D, so some of the $\sigma^{-i+1}(Y_i)$'s coincide. If $\sigma^{-i+1}(Y_i) = \sigma^{-j+1}(Y_j)$ for some $i < j$, then $Y_j = \sigma^{j-i}(Y_i)$, so $(Y_i, \ldots, Y_j)$ is a skew-cyclic train of codimension zero.

We prove the second statement of the proposition. Consider a train $(Y_1, \ldots, Y_B)$ of codimension at most $d + 1$ and length

$$B := B'(d, D) + D^{B'(d,D)}.$$

We introduce $N := D^{B'(d,D)} + 1$ trains $Z^{(1)}, \ldots, Z^{(N)}$ of length $\ell := B'(d, D)$ in $X, \sigma(X), \ldots, \sigma^{N-1}(X)$, respectively, such that, for all i, $1 \leqslant i \leqslant N$, we have

$$Z^{(i)} = \left(Z_1^{(i)}, \ldots, Z_\ell^{(i)} \right) := (Y_i, \ldots, Y_{i+\ell-1}).$$

For every i, $1 \leqslant i \leqslant N$, consider a maximal train $\widetilde{Z}^{(i)} = \left(\widetilde{Z}_1^{(i)}, \ldots, \widetilde{Z}_\ell^{(i)} \right)$ of length ℓ in $\sigma^{i-1}(X)$ containing $Z^{(i)}$. Then $\sigma^{-i+1}(\widetilde{Z}^{(i)})$ is a maximal train of length ℓ in X. If there exists i such that $\operatorname{codim} \widetilde{Z}^{(i)} \leqslant d$, then there is a skew-cyclic train of length at most $B'(d, D)$ and codimension at most d due to the definition of $B'(d, D)$. Otherwise, $\operatorname{codim} \widetilde{Z}^{(i)} = d + 1$ for every $1 \leqslant i \leqslant N$.

Corollary 6.18 implies that there are at most $D^\ell = N - 1$ maximal trains of length ℓ in X. Hence, there are a and b, $1 \leqslant a < b \leqslant N$, such that

$$\sigma^{-a+1}(\widetilde{Z}^{(a)}) = \sigma^{-b+1}(\widetilde{Z}^{(b)}).$$

Since $\operatorname{codim} \widetilde{Z}^{(a)} = \operatorname{codim} \widetilde{Z}^{(b)} = d + 1$, there exists j, $1 \leqslant j \leqslant \ell$, such that

$$\dim \widetilde{Z}_j^{(a)} = \dim \widetilde{Z}_j^{(b)} = \dim X - (d + 1).$$

Hence, since both $\widetilde{Z}_j^{(a)}$ and $Z_j^{(a)}$ are irreducible, $\dim Z_j^{(a)} \geqslant \dim X - (d+1)$ and $Z_j^{(a)} \subset \widetilde{Z}_j^{(a)}$, they are equal. Analogously, $\widetilde{Z}_j^{(b)} = Z_j^{(b)}$. Therefore,

$$\sigma^{-a+1}(Y_{a+j-1}) = \sigma^{-a+1}(Z_j^{(a)}) = \sigma^{-a+1}(\widetilde{Z}_j^{(a)})$$
$$= \sigma^{-b+1}(\widetilde{Z}_j^{(b)}) = \sigma^{-b+1}(Z_j^{(b)}) = \sigma^{-b+1}(Y_{b+j-1}).$$

Hence,

$$Y_{b+j-1} = \sigma^{b-a}(Y_{a+j-1}),$$

so, $(Y_{a+j-1}, Y_{a+j}, \ldots, Y_{b+j-1})$ is a skew-cyclic train of codimension at most $d + 1$.   □

Proposition 6.24. $B'(1, D) \leqslant \frac{D^3}{6} + \frac{D^2}{2} + \frac{4D}{3} + 1$ *for every $D \geqslant 1$.*

Proof. Let $\deg X \leqslant D$. Assume that there is no skew-cyclic train of codimension at most one in X. Let

$$X = X_1 \cup X_2 \cup \ldots \cup X_s$$

be the irreducible decomposition of X and $D_i := \deg X_i$. We construct a directed graph (with loops and multiple edges) G with vertices numbered from 1 to s as follows. For every maximal train among the marked trains of signature (i, j) in X, we draw an edge from i to j (the number of such trains is finite by Lemma 6.17). The codimension of an edge is defined to be the codimension of the corresponding train.

Case 1:   *there is a directed cycle $(c_1, \ldots, c_\ell, c_1)$ consisting of edges of codimension zero (since the graph has s vertices, there would be such a cycle with $\ell \leqslant s$). Then there is a skew-cyclic train*

$$(X_{c_1}, \sigma(X_{c_2}), \ldots, \sigma^{\ell-1}(X_{c_\ell}), \sigma^\ell(X_{c_1})),$$

of codimension zero and length at most $s + 1 \leqslant D + 1$.

Case 2:   *there is no such a directed cycle in G.* Therefore, we can reenumerate the components in such a way that $i < j$ for every codimension zero edge (i, j). Consider a train $Y = (Y_1, \ldots, Y_\ell)$ in X of length

$$\ell := \frac{D^3}{6} + \frac{D^2}{2} + \frac{4D}{3} + 1 \tag{6.8}$$

and codimension one. The train Y can be considered as a marked train with respect to a signature $\mathbf{c} = (c_1, \ldots, c_\ell)$. For every i, $1 \leqslant i < \ell$, we choose a maximal marked train T_i of signature (c_i, c_{i+1}) in X containing $(\sigma^{-i+1}(Y_i), \sigma^{-i+1}(Y_{i+1}))$ and let e_i be the edge in G corresponding to T_i. Note that

$$(e_1, \ldots, e_{\ell-1})$$

is a path in G.

Case 2a: *some edge e corresponding to a maximal train, denoted (Z_1, Z_2), of codimension one occurs twice in this path, so $e = e_i = e_j$ for some $1 \leqslant i < j < \ell$.* Without loss of generality, we may assume that

$$\dim Z_1 = \dim X - 1.$$

Since $\dim Y_i$ and $\dim Y_j$ are both at least $\dim X - 1$ and (Z_1, Z_2) is maximal, we conclude that

$$Z_1 = \sigma^{-i+1}(Y_i) = \sigma^{-j+1}(Y_j).$$

Hence, $(\sigma^{-i+1}(Y_i), \sigma^{-i+1}(Y_{i+1}), \ldots, \sigma^{-i+1}(Y_j))$ is a skew-cyclic train in X of length at most ℓ and codimension at most one.

Case 2b: *every edge of codimension one occurs in the path* $(e_1, \ldots, e_{\ell-1})$ *at most once.* Until the end of the proof, we fix the path $(e_1, \ldots, e_{\ell-1})$, and all of the quantities below are computed for this path. For an edge $e = (i, j)$, we introduce the weight $w(i, j) := i - j$. Let

$$N_+ := |\{i \mid 1 \leqslant i < \ell, \ w(e_i) \geqslant 0\}|,$$
$$N_- := |\{i \mid 1 \leqslant i < \ell, \ w(e_i) < 0\}|,$$
$$W_+ := \sum_{i=1}^{\ell-1} \max\{0, w(e_i)\}, \quad W_- := \sum_{i=1}^{\ell-1} \min\{0, w(e_i)\}.$$

By the above reenumeration, all edges with positive weight are of codimension at least one. Therefore, N_+ does not exceed the number of maximal marked trains with signatures of the form (i, j) with $i \geqslant j$. Hence, due to Lemma 6.17, we obtain

$$N_+ \leqslant \sum_{1 \leqslant j \leqslant i \leqslant s} D_i D_j.$$

Since the sum of weights along any path between vertices a and b is equal to $a - b$ and the vertices in G are numbered by the integers from 1 to s,

$$W_+ + W_- \geqslant -s + 1.$$

Combining this inequality with the fact that $N_- \leqslant -W_-$, we obtain

$$N_- \leqslant W_+ + s - 1.$$

Due to Lemma 6.17,

$$W_+ \leqslant \sum_{1 \leqslant j < i \leqslant s} (i - j) D_i D_j.$$

Thus,

$$\ell = N_+ + N_- + 1 \leqslant \sum_{1 \leqslant j \leqslant i \leqslant s} D_i D_j + \sum_{1 \leqslant j < i \leqslant s} (i - j) D_i D_j + s$$
$$\leqslant D^2 + \sum_{1 \leqslant j < i \leqslant s} (i - j - 1) D_i D_j + s. \tag{6.9}$$

For every integer $q \geqslant 1$, we introduce a function

$$f_q(z_1, \ldots, z_q) := \sum_{1 \leqslant j < i \leqslant q} (i - j - 1) z_i z_j + q.$$

We claim that, for every positive integer M, the set

$$\{f_q(z_1, \ldots, z_q) \mid q, z_1, \ldots, z_q \in \mathbb{Z}_{\geqslant 1}, \ z_1 + \ldots + z_q = M\}$$

reaches its maximum at $q = M$ and $z_1 = \ldots = z_q = 1$.

To prove the claim, consider any integer $p \geqslant 1$ and a tuple of positive integers $(w_1, \ldots, w_p)$. Let $r \leqslant p$ be an integer such that $w_r \neq 1$. We have

$$
\begin{aligned}
f_{p+1}(w_1, \ldots, w_{r-1}, w_r - 1, 1, w_{r+1}, \ldots, w_p) = \\
\sum_{j < i < r} (i - j - 1) w_i w_j + \sum_{r < j < i} (i - j - 1) w_i w_j \\
+ \sum_{j < r} w_j ((r - j - 1) w_r + 1) \\
+ \sum_{r < i} w_i ((i - r - 1) w_r + w_r - 1) + (p + 1)
\end{aligned}
\tag{6.10}
$$

and

$$
\begin{aligned}
f_p(w_1, \ldots, w_r, \ldots, w_p) = \\
\sum_{j < i < r} (i - j - 1) w_i w_j + \sum_{r < j < i} (i - j - 1) w_i w_j \\
+ \sum_{j < r < i} (i - j - 1) w_i w_j + \sum_{j < r} (r - j - 1) w_j w_r \\
+ \sum_{r < i} (i - r - 1) w_r w_i + p.
\end{aligned}
\tag{6.11}
$$

Comparing (6.10) and (6.11) term by term, we see that

$$
f_{p+1}(w_1, \ldots, w_{r-1}, w_r - 1, 1, w_{r+1}, \ldots, w_p) > f_p(w_1, \ldots, w_r, \ldots, w_p).
$$

Hence, the claim is proved. Let $\widehat{D} := D_1 + \ldots + D_s$. Combining the claim with (6.9), we obtain

$$
\begin{aligned}
\ell \leqslant D^2 + f_{\widehat{D}}(D_1, \ldots, D_s) &\leqslant D^2 + f_{\widehat{D}}(1, \ldots, 1) \\
&\leqslant D^2 + f_D(1, \ldots, 1) = D^2 + \sum_{1 \leqslant j < i \leqslant D} (i - j - 1) + D \\
&= D + D^2 + \sum_{i=1}^{D-2} i(D - 1 - i) = \frac{D^3}{6} + \frac{D^2}{2} + \frac{4D}{3}
\end{aligned}
$$

and arrive at the contradiction with the definition (6.8) of ℓ. $\qquad\square$

Propositions 6.23 and 6.24 imply

Corollary 6.25. *For all $d \in \mathbb{Z}_{\geqslant 0}$ and $D \in \mathbb{Z}_{>0}$, $B'(d, D) \leqslant B(d, D)$.*

6.3 Proof of effective Nullstellensatz

Proof of Theorem 3.1. The $\implies$ implication is straightforward, we will prove $\impliedby$. We will use the notation introduced in Section 6.2. The fact that the system consisting of 0-th, ..., $B(d, D) - 1$-th transforms of $F = 0$ considered as a polynomial system is consistent implies that $F = 0$ has a partial solution of length $B(d, D) \geqslant B'(d, D)$. Lemma 6.5 implies that there is a partial solution of the triple (X, π_1, π_2) of length $B'(d, D)$. This partial solution is a train in X of codimension $\dim X = d$ and length $B'(d, D)$. The definition of $B'(d, D)$ and Lemma 6.21 imply that there exists an infinite train in X. Then Lemma 6.5 and Corollary 6.10 imply that the system $F = 0$ has a solution in some difference ring extending k. $\qquad\square$

Proof of Corollary 3.2. The $\implies$ implication is straightforward, we will prove $\impliedby$. We will use the notation introduced in Section 6.2. If $k = \mathbb{C}$, then K can be chosen to be $\mathbb{C}$, too. A solution of the system $\{\sigma^i(F) = 0 \mid 0 \leqslant i < B(d, D)\}$ yields a partial solution of $F = 0$ of length $B(d, D)$. Analogously to the proof of Theorem 3.1, we have that the system $F = 0$ is consistent. Then Proposition 6.3 implies that $F = 0$ has a solution in $\mathbb{C}^{\mathbb{Z}}$. $\qquad\square$

6.4 Proof of effective elimination

Proof of Theorem 3.4. The $\impliedby$ implication is straightforward, we will prove $\implies$. Let $E_0 \supset E = \mathrm{Frac}(\mathrm{k}\{\mathbf{x}\})$ be any difference field extension such that E_0 is algebraically closed and has uncountable transcendence degree over the prime subfield. Since the difference ideal generated by F in $k\{\mathbf{x}, \mathbf{u}\}$ contains a nonzero polynomial depending only on $\mathbf{x}$ and their transforms, the difference ideal generated by F in $E_0\{\mathbf{u}\}$ contains 1. So, the system does not have a solution in $E_0^{\mathbb{Z}}$. Theorem 3.1 implies that the system $F = 0$ does not have a partial solution in E_0 of length $B(d, D)$. Hence, the ideal generated by $B(d, D)$ transforms of F contains 1. Since the ideal is defined over E, there is an expression of 1 over E of the form

$$1 = \sum_{i=0}^{B(d,D)-1} \sum_{j=1}^{N} c_{i,j} \sigma^i(f_j),$$

where $c_{i,j} \in E\{\mathbf{u}\}$. Multiplying both sides of the above equality by the product of the denominators of $c_{i,j}$'s, we obtain an expression of a nonzero polynomial from $k\{\mathbf{x}\}$ as a $k\{\mathbf{x}, \mathbf{u}\}$-linear combination of $B(d, D)$ transforms of F. $\qquad\square$

7 Difference Nullstellensatz over small fields

An hypothesis of our Proposition 6.3 is that the field K is uncountable. In practice, this is a harmless assumption as one might take that field to be $\mathbb{C}$. However, this result may be

conceptually unsatisfactory, and one might wish to find solutions to difference equations in sequences taken from a small field, such as the field of algebraic numbers.

With the next proposition, we show how to weaken the uncountability hypothesis by appealing to a more refined equivalent condition to the consistency of a system of difference equations coming from our work towards the effective Nullstellensatz and a theorem of Hrushovski on the limit theory of the Frobenius automorphisms [18]. Our invocation of Hrushovski's theorem is essentially contained in Fakhruddin's proof of the density of periodic points for polarized algebraic dynamical systems in [12]. For our purposes a slightly weaker result due to Varshavsky [38] suffices.

Theorem 7.1. *For all algebraically closed inversive difference fields K (without any restriction on the cardinality) and finite sets $F \subseteq K\{x_1, \ldots, x_n\}$, the following statements are equivalent:*

1. *F has a solution in $K^{\mathbb{Z}}$.*

2. *F has a solution in $K^{\mathbb{N}}$.*

3. *F has finite partial solutions in K^N for all $N \gg 0$.*

4. *The ideal $[F] := \langle \{\sigma^j(F) \mid j \in \mathbb{N}\} \rangle \subseteq K\{x_1, \ldots, x_n\}$ does not contain 1.*

5. *The ideal $[F]^* := \langle \{\sigma^j(F) \mid j \in \mathbb{Z}\} \rangle \subseteq K\{x_1, \ldots, x_n\}^*$ does not contain 1.*

6. *F has a solution in some difference K-algebra.*

In order to prove Theorem 7.1, we will extract two consequences of [38]. In Lemma 7.2 and 7.3, ϕ_s denotes the s-th power of the Frobenius automorphism.

Lemma 7.2. *For every finitely generated difference subring R of a difference field K, there exist a prime p, a positive integer s, and a difference homomorphism $\psi \colon R \to \mathbb{F}$, where $\mathbb{F}$ is the algebraic closure of $\mathbb{F}_p$ considered as a difference ring with respect to ϕ_s.*

Proof. The proof will proceed in two steps.

Step 1: We will show that there exists a prime p and a difference field L of characteristic p such that there exists a homomorphism $R \to L$ of difference rings. If $\operatorname{char} K > 0$, then we can take L to be K. Let now $\operatorname{char} K = 0$ and R generated by $a_1, \ldots, a_\ell$. Since R is a difference subring of a difference field, the ideal

$$I := \{f \in \mathbb{Z}\{x_1, \ldots, x_\ell\} \mid f(a_1, \ldots, a_\ell) = 0\} \tag{7.1}$$

is a perfect difference ideal [6, p. 76, §12]. As such, because every finitely generated difference ring is a Ritt difference ring [6, Chapter 3, Theorems II, and V], I

is finitely generated as a perfect difference ideal. Let $g_1, \ldots, g_s \in \mathbb{Z}\{x_1, \ldots, x_\ell\}$ be a finite set of such generators. Consider a model of ACFA_0 containing K. Then the sentence

$$\varphi := \exists \mathbf{x} \, (g_1(\mathbf{x}) = \ldots = g_s(\mathbf{x}) = 0)$$

is true in this model. [5, (1.6), 2nd paragraph] implies that there exists a finite disjunction, say ψ, of sentences specifying (up to an isomorphism) a difference field structure on some Galois extensions of the prime subfield such that

- φ and ψ are equivalent in ACFA_0. In particular, ψ holds in some model of ACFA_0.

- There exists a positive integer N such that, for every prime $p > N$, φ and ψ are equivalent in ACFA_p.

Applying the Chebotarev density theorem as in [5, (1.14)], one can show that, since ψ is consistent with ACFA_0, there are inifinitely many primes p such that ψ holds in some model of ACFA_p. We fix such p that is greater than N and a model L of ACFA_p in which ψ and, consequently, φ hold. Then there are $b_1, \ldots, b_\ell \in L$ such that $g_1(b_1, \ldots, b_\ell) = \ldots = g_s(b_1, \ldots, b_\ell) = 0$. Then the kernel of a difference homomorphism $\mathbb{Z}\{x_1, \ldots, x_\ell\} \to L$ defined by $x_i \mapsto b_i$ contains I, so it yields a difference homomorphism $R \to L$.

Step 2:   If $\mathrm{char}\, K = 0$, we replace K with L and R with its image in L. Thus, in what follows, we assume that $\mathrm{char}\, K = p > 0$. Let h be the maximum of the orders of $g_1, \ldots, g_s$. Let $b_1, \ldots, b_N$ be the elements of

$$\{\sigma^j(a_i) \mid 1 \leqslant i \leqslant \ell, 0 \leqslant j < h\}$$

written in some order, so $N = \ell h$. Then R is also generated by $b_1, \ldots, b_N$ as a difference ring, and the corresponding vanishing ideal in the difference polynomial ring $\mathbb{Z}\{y_1, \ldots, y_N\}$ is generated as a perfect difference ideal by difference polynomials of order one. Replacing $a_1, \ldots, a_\ell$ by $b_1, \ldots, b_N$, we may assume that I, defined in (7.1), is generated as a perfect difference ideal by order one difference polynomials.

Let $\mathfrak{q} \subseteq \mathbb{F}_p[x_1, \ldots, x_\ell, y_1, \ldots, y_\ell]$ be the ideal of all polynomials vanishing on $(a_1, \ldots, a_\ell, \sigma(a_1), \ldots, \sigma(a_\ell))$. Since $a_1, \ldots, a_\ell$ are elements of a difference field, the ideals

$$\mathfrak{p}_1 := \mathfrak{q} \cap \mathbb{F}_p[\mathbf{x}] \quad \text{and} \quad \mathfrak{p}_2 := \mathfrak{q} \cap \mathbb{F}_p[\mathbf{y}]$$

are transformed one to the other under the substitution $\mathbf{x} \mapsto \mathbf{y}$. Then

$$X := \mathrm{Spec}(\mathbb{F}_p[\mathbf{x}]/\mathfrak{p}_1) = \mathrm{Spec}(\mathbb{F}_p[\mathbf{y}]/\mathfrak{p}_2) \quad \text{and} \quad C := \mathrm{Spec}(\mathbb{F}_q[\mathbf{x}, \mathbf{y}]/\mathfrak{q})$$

are irreducible schemes of finite type over $\mathbb{F}_p$, and C is a subset of $X \times X$. Then, by [38, Theorem 0.1], there exists a positive integer s such that the intersection of C with the graph of ϕ_s in $\mathbb{F}^{2\ell}$ is nonempty, where $\mathbb{F}$ is the algebraic closure of $\mathbb{F}_p$. Let $(a_1^*, \ldots, a_\ell^*, \phi_s(a_1^*), \ldots, \phi_s(a_\ell^*))$ be a point in the intersection. Since the substitution $\sigma^j(x_i) = \phi_s^j(a_i^*)$ annihilates q, it also annihilates every polynomial in its perfect closure $I \pmod{p}$. Then the map $\psi \colon R \to \mathbb{F}$ defined by $\psi\left(\sigma^j(a_i)\right) = \phi_s^j(a_i^*)$ is a desired homomorphism of difference rings (R, σ) and $(\mathbb{F}, \phi_s)$. $\qquad\square$

Lemma 7.3. *For every*

- *prime number p,*

- *positive integer s,*

- *scheme X of finite type defined over $\mathbb{F}$, the algebraic closure of $\mathbb{F}_p$,*

- *irreducible subvariety $\Gamma \subset X \times \phi_s(X)$ such that the projections to X and $\phi_s(X)$ are dominant,*

there exists an infinite sequence $(a_i)_{i=-\infty}^{\infty}$ such that $(a_i, a_{i+1}) \in \phi_{si}(\Gamma)$ for every $i \in \mathbb{Z}$.

Proof. Since X and Γ are defined over some finite subfield of $\mathbb{F}$, there is a positive integer ℓ with $\phi_{s\ell}(X) = X$ and $\phi_{s\ell}(\Gamma) = \Gamma$. Lemma 6.13 implies that there exists an irreducible component Ξ of the fiber product

$$\Gamma \times_{\phi_s(X)} \phi_s(\Gamma) \times_{\phi_{2s}(X)} \cdots \times_{\phi_{(\ell-1)s}(X)} \phi_{(\ell-1)s}(\Gamma).$$

such that the projections of Ξ onto $\Gamma, \phi_s(\Gamma), \ldots, \phi_{(\ell-1)s}(\Gamma)$ are dominant. We denote the projection $\Xi \to \phi_{si}(\Gamma)$ by ρ_i for every $0 \leqslant i \leqslant \ell - 1$.

Let $\tau_1 \colon \Gamma \to X$ and $\tau_2 \colon \Gamma \to \phi_s(X)$ denote the projections. We define projections $\pi_i \colon \Xi \to \phi_{si}(X)$ for $0 \leqslant i \leqslant \ell$ as follows:

$$\pi_i = \begin{cases} \tau_1 \circ \rho_0, & \text{for } i = 0, \\ \tau_1 \circ \rho_i = \tau_2 \circ \rho_{i-1}, & \text{for } 0 < i < \ell, \\ \tau_2 \circ \rho_{\ell-1}, & \text{for } i = \ell. \end{cases}$$

Note that the π_i's are dominant. Consider the fiber product of $\Xi \times_X \Xi$ where the first $\Xi \to X$ is π_ℓ and the second map $\Xi \to X$ is π_0. Lemma 6.13 implies that there exists an irreducible component Υ of this product such that the projections of Υ onto both Ξ's are dominant. Take r so that Ξ and Υ are both defined over $\mathbb{F}_{p^r}$ and

$$s\ell \mid r.$$

By [38, Theorem 0.1], there is a power ϕ_t of ϕ_r and a point $a = (a_0, \ldots, a_{\ell-1}) \in \Xi(\mathbb{F})$ with $(a, \phi_t(a)) \in \Upsilon(\mathbb{F})$. Note that ϕ_t leaves invariant Γ, Ξ, and Υ. Since coefficients of

the π_i's and ρ_j's are invariant under ϕ_1, we will denote the conjugation of any of these maps by any power of ϕ_1 by the same letter. For $0 \leq i < \ell$ and $j \in \mathbb{Z}$, define

$$a_{i+j\ell} := \pi_i(\phi_{tj}(a)).$$

Let us show that the sequence $\{a_i\}_{i=-\infty}^{\infty}$ satisfies the requirement of the lemma. Consider $j \in \mathbb{Z}$ and $0 \leqslant i < \ell$. Then $a_{i+j\ell} = \tau_1(\rho_i(\phi_{tj}(a)))$. We also have

$$a_{i+j\ell+1} = \tau_1(\rho_{i+1}(\phi_{tj}(a))) = \tau_2(\rho_i(\phi_{tj}(a))) \text{ for } i < \ell - 1,$$
$$a_{i+j\ell+1} = \tau_1(\rho_0(\phi_{t(j+1)}(a))) = \tau_2(\rho_{\ell-1}(\phi_{tj}(a))) \text{ for } i = \ell - 1$$

because Ξ and Υ are components of the corresponding fiber products. In both cases,

$$(a_{i+j\ell}, a_{i+j\ell+1}) \in \rho_i(\phi_{tj}(\Xi)) = \rho_i(\Xi) \subset \phi_{si}(\Gamma) = \phi_{s(i+j\ell)}(\Gamma). \qquad \square$$

In Lemmas 7.4 and 7.5, for a valued field (K, v), we write

$$\mathcal{O} = \{x \in K \ : \ v(x) \geqslant 0\}$$

for the valuation ring,

$$\mathfrak{m} = \{x \in K \ : \ v(x) > 0\}$$

for the maximal ideal of $\mathcal{O}$, and $k = \mathcal{O}/\mathfrak{m}$ for the residue field. We denote the reduction map $r : \mathcal{O} \to k$ by r and will abuse notation writing r for the reduction map on associated objects.

Lemma 7.4. *Let (K, v) be a Henselian field, $n \leqslant m$ positive integers, $f_1, \ldots, f_n \in \mathcal{O}[x_1, \ldots, x_m]$ and $a = (a_1, \ldots, a_m) \in k^m$. We assume that, for each i, we have $r(f_i)(a) = 0$ and that the matrix $\left(\frac{\partial r(f_i)}{\partial x_j}(a) \right)_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m}$ has rank n. Then there is $c = (c_1, \ldots, c_m) \in \mathcal{O}^m$ such that $f_1(c) = \ldots = f_n(c) = 0$ and $r(c) = a$.*

Proof. By hypothesis, there is some $J \subseteq \{x_1, \ldots, x_m\}$ with $|J| = n$ and invertible matrix $\left(\frac{\partial r(f_i)}{\partial x_j}(a) \right)_{1 \leqslant i \leqslant n, j \in J}$. Relabeling the variables, we may assume that $J = \{1, \ldots, n\}$. Define $f_i := x_i$ for $n < i \leq m$. Then the square matrix $\left(\frac{\partial r(f_i)}{\partial x_j}(a) \right)_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n}$ is invertible. There exists some $b \in \mathcal{O}^m$ such that $r(b) = a$. Then, by to [24, Section 4, Multidimensional Hensel's Lemma], there is some $c \in \mathcal{O}^n$ with $f_1(c) = \cdots = f_n(c) = 0$ and $r(c) = r(a)$. $\qquad \square$

Lemma 7.5. *Let (K, v) be a Henselian field and $f : X \to Y$ a smooth map of schemes of finite type over $\mathcal{O}$. Suppose that $a \in X(k)$ and $b \in Y(\mathcal{O})$ satisfy $f(a) = r(b)$. Then there is a point $c \in X(\mathcal{O})$ with $f(c) = b$ and $r(c) = a$.*

Proof. [33, Tag 01V7] implies that there are affine open neighborhoods $U \subseteq X$ and $V \subseteq Y$ of a and $r(b)$, respectively, for which $f_U \colon U \to V$ is standard smooth. That is, there exist:

- positive integers m and n,

- a finitely generated $\mathcal{O}$-algebra S such that $V = \mathrm{Spec}(S)$,

- polynomials $g_1, \ldots, g_n \in S[x_1, \ldots, x_m]$ such that $U = \mathrm{Spec}(T)$, where $T = S[x_1, \ldots, x_m]/(g_1, \ldots, g_n)$,

such that

- some $n \times n$ minor of the Jacobian $\left(\frac{\partial g_i}{\partial x_j} \right)$ is an invertible element of T and

- f_U is the dual morphism of schemes to the natural homomorphism $S \to T$.

Since $\mathcal{O}$ is a local ring and $r(b)$ is a reduction of b modulo $\mathfrak{m} \subset \mathcal{O}$, the point b belongs to any open neighborhood of $r(b)$, in particular, $b \in V(\mathcal{O})$. This corresponds to an $\mathcal{O}$-algebra homomorphism $b^\sharp \colon S \to \mathcal{O}$. Let $a^\sharp$ denote the $\mathcal{O}$-algebra homomorphism $\mathcal{O}[U] \to k$ corresponding to $a \in U(k)$.

For each i, $1 \leqslant i \leqslant n$, consider the polynomials $b^\sharp(g_i) \in \mathcal{O}[x_1, \ldots, x_m]$ and $a^\sharp(g_i) \in k[x_1, \ldots, x_m]$ that are obtained from g_i by applying $b^\sharp$ and $a^\sharp$, respectively, to the coefficients. The fact $r(b) = f(a)$ implies that $r\left(b^\sharp(g_i)\right) = a^\sharp(g_i)$. Let a_j be the result of applying $a^\sharp$ to the image of x_j in T for $1 \leqslant j \leqslant m$. Since $a^\sharp$ is a homomorphism, $a^\sharp(g_i)(a_1, \ldots, a_m) = 0$ for every $1 \leqslant i \leqslant n$ and also the Jacobian matrix $\left(\frac{\partial a^\sharp(g_i)}{\partial x_j} \right)$ has full rank at $(a_1, \ldots, a_m)$.

Then, by Lemma 7.4, we may find $(c_1, \ldots, c_m) \in \mathcal{O}^m$ for which $b^\sharp(g_i)(c_1, \ldots, c_m) = 0$ for $1 \leqslant i \leqslant n$ and $r(c_j) = a_j$ for $1 \leqslant j \leqslant m$. Since $b^\sharp(g_i)(c_1, \ldots, c_m) = 0$ for $1 \leqslant i \leqslant n$, the map $c^\sharp \colon T \to \mathcal{O}$ defined by $c^\sharp|_S = b^\sharp$ and by $c^\sharp(x_i) = c_i$ for $1 \leqslant i \leqslant m$ is a well-defined $\mathcal{O}$-algebra homomorphism. This gives us a point $c \in U(\mathcal{O})$ such that $f(c) = b$. Moreover, $r(c) = a$ since $r(c_i) = a_i$ for every $1 \leqslant i \leqslant m$. $\qquad\square$

Corollary 7.6. *Let (K, v) be a Henselian field and X a scheme of finite type over $\mathcal{O}$ such that the canonical morphism $X \to \mathrm{Spec}(\mathcal{O})$ is smooth. Then, for every $a \in X(k)$, there exists $c \in X(\mathcal{O})$ such that $r(c) = a$.*

Proof. The corollary follows from Lemma 7.5 applied to $Y = \mathrm{Spec}(\mathcal{O})$ and b being the identity map $\mathrm{Spec}(\mathcal{O}) \to \mathrm{Spec}(\mathcal{O})$. $\qquad\square$

With these statements in place, we finish the proof of Theorem 7.1.

In what follows, for a positive integer m and a commutative ring R, R^m denotes the commutative ring generated by the set $\{r^m \,|\, r \in R\}$. For an affine scheme X over a perfect

ring R of characteristic p and $q = p^n$, we define a scheme $X^{(q)}$ by $X^{(q)} := \mathrm{Spec}(\mathcal{O}_X^q)$. There is a map $F_n \colon X \to X^{(q)}$ that is dual to the inclusion $\mathcal{O}_X^q \hookrightarrow \mathcal{O}_X$. This map is a special case of what is called the relative Frobenius morphism. See [33, Tag 0CC6] for more details. If R is perfect, F_n defines a bijection between $X(R)$ and $X^{(q)}(R)$. If $p = 0$, we will assume that $q = 1$ and F_n is the identity map.

Lemma 7.7. *If $\mu \colon \Gamma \to Z$ is morphism of irreducible affine varieties over an algebraically closed field K, then there exist*

- *an affine variety Υ,*

- *morphisms $\nu \colon \Gamma \to \Upsilon$ and $\tau \colon \Upsilon \to Z$,*

- *a positive integer n and a morphism $\gamma \colon \Upsilon \to \Gamma^{(q)}$, where $q = p^n$,*

such that $\mu = \tau \circ \nu$, $\gamma \circ \nu = F_n$, ν is finite, and τ is generically smooth.

Proof. If $\mathrm{char}\, K = 0$, take $\Upsilon = \Gamma$, $\nu = \mathrm{id}_\Gamma$ and $\tau = \mu$ by [32, Theorem 2.27].

Let $\mathrm{char}\, K = p > 0$, $t_1, \ldots, t_\ell$ be a transcendence basis of $K(\Gamma)$ over $E := \mathrm{Quot}(\mu^*(\mathcal{O}_Z))$, and L be the relative separable closure of $E(t_1, \ldots, t_\ell)$ in $K(\Gamma)$. Then, as $K(\Gamma)$ is a finite purely inseparable extension of L, for $n \gg 0$ we have $K(\Gamma)^{p^n} \subseteq L$. Let $q := p^n$ and $A = \mu^*(\mathcal{O}_Z)[\mathcal{O}_\Gamma^q]$, the ring generated by $\mu^*(\mathcal{O}_Z)$ and $\mathcal{O}_\Gamma^q$. Set $\Upsilon := \mathrm{Spec}(A)$ over K.

Dual to the homomorphisms of rings $\mathcal{O}_Z \to A$ and $A \to \mathcal{O}_\Gamma$, we have morphisms $\tau \colon \Upsilon \to Z$ and $\nu \colon \Gamma \to \Upsilon$ with $\mu = \tau \circ \nu$. Since the field extensions $E \hookrightarrow K(\Upsilon)$ is a subextension of the the separable extension $E \hookrightarrow L$, the morphism $\tau \colon \Upsilon \to Z$ is smooth at the generic point of Υ due to [33, Tag 07ND]. Form the inclusion $\mathcal{O}_\Gamma^q \hookrightarrow A = \mathcal{O}_\Upsilon$, we obtain the morphism $\gamma \colon \Upsilon \to \Gamma^{(q)}$ with $F_n = \gamma \circ \nu$.

Since $\mathcal{O}_\Gamma^q \subset \mathcal{O}_\Gamma$ is a finite integral extension and $\mathcal{O}_\Gamma^q \subset A \subset \mathcal{O}_\Gamma$, the extension $A \subset \mathcal{O}_\Gamma$ is also a finite integral extension. Hence, the dual map $\nu \colon \Gamma \to \Upsilon$ is a finite morphism. $\qquad\qquad\square$

Proof of Theorem 7.1. The only implication whose proof in the original argument for Proposition 6.3 used uncountability is from 5. to 1. We observe that 5. implies 3., because 1 is not contained in any ideal generated by finitely many transforms of the system, so Hilbert's Nullstellensatz implies that there exist arbitrarily long partial solutions of the system over K. This is exactly 3.

Consider the triple (X, π_1, π_2) constructed in Section 6.2. Due to Lemma 6.5, item 3 implies that (X, π_1, π_2) has arbitrarily long partial solutions. On the other hand, the existence of a solution to $F = 0$ in $K^{\mathbb{Z}}$ is equivalent to the existence of a two-sided infinite solution to (X, π_1, π_2) over K (see Lemma 6.5). We thus reduce to finding a solution to

(X, π_1, π_2) over K. Then Proposition 6.23 implies that there exists an infinite skew-cyclic train

$$(\ldots, Y_1, Y_2, \ldots, Y_\ell, \sigma^\ell(Y_1), \ldots) \tag{7.2}$$

in X. Let $\mathbf{c}$ be a signature of the train $(Y_1, \ldots, Y_\ell)$ and let $Y \subset W_\mathbf{c} \subset X^\mathbf{c}$ be the associated irreducible variety given by Lemma 6.16. For $1 \le i \le \ell$, let $\rho_i \colon Y \to Y_i$ be the dominant projection to Y_i (which is $\psi_{\ell,i}|_Y$ in the notation of Lemma 6.16). The projection $\sigma^j(Y) \to \sigma^j(Y_i)$ obtained by conjugation by σ^j of ρ_i will be denoted by $\sigma^j(\rho_i)$ for every $j \in \mathbb{Z}$. Recall that, since (7.2) is a train, $\pi_2 \circ \rho_\ell$ and $\pi_1 \circ \sigma^\ell(\rho_1)$ are dominant onto the same variety. Due to Lemma 6.13, there exists an irreducible component Γ, which we fix, of the fiber product of Y with $\sigma^\ell(Y)$ over $\pi_2 \circ \rho_\ell$ and $\pi_1 \circ \sigma^\ell(\rho_1)$ such that $\mu_1 : \Gamma \to Y$ and $\mu_2 : \Gamma \to \sigma^\ell(Y)$ are dominant.

Let us call a sequence $(a_i)_{i=-\infty}^{\infty}$ with $a_i \in \sigma^{i\ell}(Y)$ and $(a_i, a_{i+1}) \in \sigma^{i\ell}(\Gamma)$ for all i a *weak solution* to (Y, Γ). Such a weak solution gives rise to the solution

$$(\ldots, \sigma^{-\ell}(\rho_1)(a_{-1}), \ldots, \sigma^{-\ell}(\rho_\ell)(a_{-1}), \rho_1(a_0), \rho_2(a_0), \ldots, \rho_\ell(a_0), \sigma^\ell(\rho_1)(a_1), \ldots, \sigma^\ell(\rho_\ell)(a_1), \ldots)$$

of (X, π_1, π_2). Thus, it suffices for us to find a weak solution. Lemma 7.7 implies that there exist

- Υ_1 and Υ_2 be affine varieties

- n a positive integer,

- $\nu_i \colon \Gamma \to \Upsilon_i$, $\tau_i \colon \Upsilon_i \to Y$, $\gamma_i \colon \Upsilon_i \to \Gamma^{(q)}$, morphisms, where $q = p^n$ and $i = 1, 2$,

so that, for $i = 1, 2$,

- $\gamma_i \circ \nu_i = F_n$,

- τ_i is generically smooth,

- $\mu_i = \tau_i \circ \nu_i$.

We fix some equations defining Γ, Y, Υ_i, γ_i, τ_i, ν_i, and μ_i for $i = 1, 2$. Denote the difference ring generated by the coefficients of these equations by R. Let $\pi \colon \Gamma^{(q)} \to \operatorname{Spec}(R)$ be the dual to the natural embedding $R \to \mathcal{O}_\Gamma^q$. [33, Tag 07ND] implies that π is generically smooth. Let Γ, Y, Υ_1, and Υ_2 be the models of Γ, Y, Υ_1, and Υ_2 defined by

these fixed equations over R. Thus, we have the following diagram:
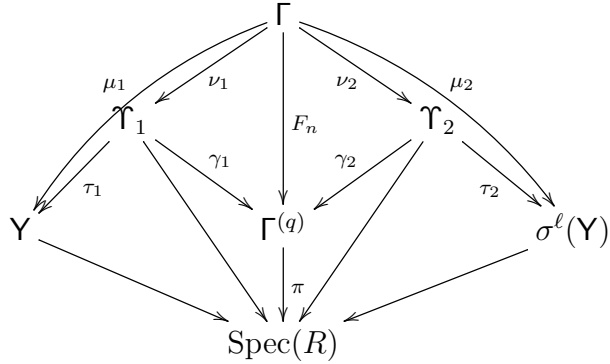
Let $\hat{\Upsilon}_1$, $\hat{\Upsilon}_2$, and $\hat{\Gamma}^{(q)}$ be dense open subsets in Υ_1, Υ_2, and $\Gamma^{(q)}$, respectively, such that τ_1, τ_2, and π, respectively, are smooth on these subsets, which exist since smoothness of a morphism is an open condition (see the discussion just after [33, Tag 01V5]). Let

$$\widetilde{\Gamma} = \nu_1^{-1}(\hat{\Upsilon}_1) \cap \nu_2^{-1}(\hat{\Upsilon}_1) \cap F_n^{-1}(\hat{\Gamma}^{(q)}),$$

which is dense open in Γ. Let Γ' be a non-empty open subset of $\widetilde{\Gamma}$ defined by a single inequality $f \neq 0$, where $f \in \mathcal{O}_\Gamma$. The image of Γ' under F_n is open dense in $(\Gamma')^{(q)} \subset \Gamma^{(q)}$, defined by $f^q \neq 0$. Let

$$\Upsilon'_i = \gamma_i^{-1}\left((\Gamma')^{(q)}\right) \cap \hat{\Upsilon}_i, \quad i = 1, 2.$$

Then $\nu_i(\Gamma') \subset \Upsilon'_i$, and $(\Gamma')^{(q)} \subset \hat{\Gamma}^{(q)}$.

We apply Lemma 7.2 to (R, σ^ℓ) and obtain $\psi \colon (R, \sigma^\ell) \to (\mathbb{F}, \phi_s)$, where $\mathbb{F}$ is the algebraic closure of $\mathbb{F}_p$ and, in the case $\operatorname{char} K = 0$, p is some prime number provided by Lemma 7.2. Let $X_\mathbb{F}$ denote the base change of a scheme X over R to $\mathbb{F}$ via ψ. Let $(a_i)_{i=-\infty}^{\infty}$ be a sequence such that, for each $i \in \mathbb{Z}$,

$$(a_i, a_{i+1}) \in \phi_{si}(\Gamma'_\mathbb{F})(\mathbb{F}).$$

Such a sequence exists by Lemma 7.3. Fix an extension of ψ to a place ϑ on K (see [11, Theorem 3.1.1]). Let $\mathcal{O}$ be the valuation ring of ϑ and v be a valuation on K. Note that $R \subset \mathcal{O}$. Also note that we do not assert that ϑ respects σ on all of $\mathcal{O}$ nor even that $\mathcal{O}$ is preserved by σ. Let $\mathbb{E}$ be the residue field of $\mathcal{O}$. Since K is algebraically closed, $\mathbb{E}$ is also algebraically closed [11, Theorem 3.2.11]. Since $\mathbb{F}_p \subset \mathbb{E}$, $\mathbb{F}$ is embedded into $\mathbb{E}$.

[33, Tag 01VB] implies that the morphisms of schemes $(\Upsilon'_1)_\mathcal{O} \to Y_\mathcal{O}$, $(\Upsilon'_2)_\mathcal{O} \to \sigma^\ell(Y)_\mathcal{O}$, and $(\Gamma')^{(q)}_\mathcal{O} \to \operatorname{Spec}(\mathcal{O})$ are smooth as well as all their shifts/conjugations by σ^ℓ. We shall now build a weak solution $(b_i)_{i=-\infty}^{\infty}$ to $(Y_\mathcal{O}(\mathcal{O}), \Gamma'_\mathcal{O}(\mathcal{O}))$ so that

$$\forall\, i \in \mathbb{Z} \ \ \vartheta(b_i) = a_i.$$

Since K is algebraically closed, (K, v) is Henselian [24, Lemma 4.1]. For $i = 0$ and $i = 1$, since $\pi\colon (\Gamma')_{\mathcal{O}}^{(q)} \to \mathrm{Spec}(\mathcal{O})$ is smooth, every point in $(\Gamma')_{\mathbb{F}}^{(q)}(\mathbb{F})$ lifts to a point in $(\Gamma')_{\mathcal{O}}^{(q)}(\mathcal{O})$ due to Corollary 7.6. Thus, we may choose some $(\hat{b}_0, \hat{b}_1) \in (\Gamma')_{\mathcal{O}}^{(q)}(\mathcal{O})$ specializing to $(F_n(a_0), F_n(a_1))$ and set $b_0 = F_n^{-1}(\hat{b}_0)$ and $b_1 = F_n^{-1}(\hat{b}_1)$.

Assume that we have already constructed b_i for some $i > 0$ so that $\vartheta(b_i) = a_i$. Due to Lemma 7.5 applied to the morphism of schemes

$$\sigma^{i\ell} \circ \tau_1 \circ \sigma^{-i\ell} : \sigma^{i\ell}\left((\Upsilon_1')_{\mathcal{O}}\right) \to \sigma^{i\ell}\left(\mathsf{Y}_{\mathcal{O}}\right)$$

and points $\left(\sigma^{i\ell} \circ \nu_1 \circ \sigma^{-i\ell}\right)((a_i, a_{i+1}))$ and b_i, there exists $P \in \sigma^{i\ell}\left((\Upsilon_1')_{\mathcal{O}}\right)$ such that

$$(\sigma^{i\ell} \circ \tau_1 \circ \sigma^{-i\ell})(P) = b_i \quad \text{and} \quad \vartheta(P) = \left(\phi_s^i \circ \nu_1 \circ \phi_s^{-i}\right)((a_i, a_{i+1})).$$

Consider

$$Q = F_n^{-1}\left(\sigma^{i\ell} \circ \gamma_1 \circ \sigma^{-i\ell}(P)\right) \in \sigma^{i\ell}\left(\Gamma_{\mathcal{O}}'(\mathcal{O})\right).$$

Since ν_1 is a finite morphism, it is surjective on $\mathcal{O}$-points due to [32, Theorem 1.12] together with [11, Theorem 3.1.3]. Using this and the fact that F_n is bijective on $\mathcal{O}$-points, $\sigma^{i\ell} \circ \nu_1 \circ \sigma^{-i\ell}(Q) = P$. Hence,

$$(\sigma^{i\ell} \circ \mu_1 \circ \sigma^{-i\ell})(Q) = (\sigma^{i\ell} \circ \tau_1 \circ \sigma^{-i\ell})(P) = b_i,$$

so Q can be written as (b_i, c). Since

$$F_n^{-1} \circ \phi_s^i \circ \gamma_1 \circ \nu_1 \circ \phi_s^{-i} = \phi_s^i \circ F_n^{-1} \circ \gamma_1 \circ \nu_1 \circ \phi_s^{-i} = \phi_s^i \circ \mathrm{id} \circ \phi_s^{-i} = \mathrm{id},$$

we have

$$\vartheta(Q) = F_n^{-1} \circ \phi_s^i \circ \gamma_1 \circ \nu_1 \circ \phi_s^{-i}\left((a_i, a_{i+1})\right) = (a_i, a_{i+1}).$$

Thus, we can set $b_{i+1} = c$. In the same way, we produce the b_i with $i < 0$ using the fact that $(\Upsilon_2')_{\mathcal{O}} \to \sigma^\ell(\mathsf{Y})_{\mathcal{O}}$ is smooth. $\qquad\square$

References

[1] Allen, L.: Some discrete-time *SI*, *SIR*, and *SIS* epidemic models. Mathematical Biosciences **124**(1), 83–105 (1994). URL http://dx.doi.org/10.1016/0025-5564(94)90025-6

[2] Bates, D.J., Hauenstein, J.D., Sommese, A.J., Wampler, C.W.: Numerically Solving Polynomial Systems with Bertini, *Software, Environments, and Tools*, vol. 25. SIAM, Philadelphia, PA (2013)

[3] Binyamini, G.: Bezout-type theorems for differential fields. Compositio Mathematica **153**(4), 867–888 (2017). URL http://dx.doi.org/10.1112/S0010437X17007035

[4] Brownawell, W.D.: Bounds for the degrees in the Nullstellensatz. Annals of Mathematics **126**(3), 577–591 (1987). URL http://dx.doi.org/10.2307/1971361

[5] Chatzidakis, Z., Hrushovski, E.: Model theory of difference fields. Transactions of the American Mathematical Society **351**(8), 2997–3071 (1999). URL http://dx.doi.org/10.1090/S0002-9947-99-02498-8

[6] Cohn, R.: Difference Algebra. Interscience Publishers John Wiley & Sons, New York-London-Sydeny (1965)

[7] Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. Undergraduate Texts in Mathematics. Springer, New York (2015). URL http://dx.doi.org/10.1007/978-3-319-16721-3

[8] Cushing, J., Henson, S., Roeger, L.: Coexistence of competing juvenile-adult structured populations. Journal of Biological Dynamics **1**(2), 201–231 (2007). URL http://dx.doi.org/10.1080/17513750701201372

[9] D'Alfonso, L., Jeronimo, G., Solernó, P.: Effective differential Nullstellensatz for ordinary DAE systems over the complex numbers. Journal of Complexity **30**(5), 588–603 (2014). URL http://dx.doi.org/10.1016/j.jco.2014.01.001

[10] Ekhad, S.B., Zeilberger, D.: How to generate as many Somos-like miracles as you wish. Journal of Difference Equations and Applications **20**, 852–858 (2014). URL http://dx.doi.org/10.1080/10236198.2013.823956

[11] Engler, A.J., Prestel, A.: Valued Fields. Springer-Verlag, Berlin, Heidelberg (2005). URL http://dx.doi.org/10.1007/3-540-30035-X

[12] Fakhruddin, N.: Questions on self maps of algebraic varieties. Journal of the Ramanujan Mathematical Society **18**(2), 109–122 (2003)

[13] Gao, X.S., van der Hoeven, J., Yuan, C.M., Zhang, G.L.: Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation **44**(9), 1137–1163 (2009). URL http://dx.doi.org/10.1016/j.jsc.2008.02.010

[14] Gao, X.S., Luo, Y., Yuan, C.: A characteristic set method for ordinary difference polynomial systems. Journal of Symbolic Computation **44**(3), 242–260 (2009). URL doi.org/10.1016/j.jsc.2007.05.005

[15] Harris, J.: Algebraic Geometry: A First Course. Springer (1992). URL http://dx.doi.org/10.1007/978-1-4757-2189-8

[16] Heintz, J.: Definability and fast quantifier elimination in algebraically closed fields. Theoretical Computer Science **24**(3), 239–277 (1983). URL http://dx.doi.org/10.1016/0304-3975(83)90002-6

[17] Hong, H., Ovchinnikov, A., Pogudin, G., Yap, C.: Global identifiability of differential models (2018). URL https://arxiv.org/abs/1801.08112. Preprint

[18] Hrushovski, E.: The elementary theory of the Frobenius automorphism. URL http://www.ma.huji.ac.il/~ehud/FROB.pdf

[19] Hrushovski, E.: The Manin-Mumford conjecture and the model theory of difference fields. Annals of Pure and Applied Logic **112**(1), 43–115 (2001). URL https://doi.org/10.1016/S0168-0072(01)00096-3

[20] Hrushovski, E., Pillay, A.: Effective bounds for the number of transcendental points on subvarieties of semi-abelian varieties. American Journal of Mathematics **122**(3), 439–450 (2000). URL http://dx.doi.org/10.1353/ajm.2000.0020

[21] Hrushovski, E., Point, F.: On von Neumann regular rings with an automorphism. Journal of Algebra **315**(1), 76–120 (2007). URL http://dx.doi.org/10.1016/j.jalgebra.2007.05.006

[22] Jelonek, Z.: On the effective Nullstellensatz. Inventiones Mathematicae **162**(1), 1–17 (2005). URL http://dx.doi.org/10.1007/s00222-004-0434-8

[23] Kollár, J.: Sharp effective Nullstellensatz. Journal of the Americal Mathematical Society **1**(4), 963–975 (1988). URL http://dx.doi.org/10.1090/S0894-0347-1988-0944576-7

[24] Kuhlmann, F.V.: Valuation theoretic and model theoretic aspects of local uniformization. In: Resolution of singularities, *Progr. Math.*, vol. 181, pp. 381–456. Birkhäuser, Basel (2000). URL http://dx.doi.org/10.1007/978-3-0348-8399-3_15

[25] Levin, A.: Difference Algebra. Springer (2008). URL http://dx.doi.org/10.1007/978-1-4020-6947-5

[26] Li, W., Li, Y.H.: Difference Chow form. Journal of Algebra **428**, 67–90 (2015). URL https://doi.org/10.1016/j.jalgebra.2014.12.037

[27] Li, W., Yuan, C.M., Gao, X.S.: Sparse difference resultant. Journal of Symbolic Computation **68**, 169–203 (2015). URL https://doi.org/10.1016/j.jsc.2014.09.016

[28] Lyzell, C., Glad, T., Enqvist, M., Ljung, L.: Difference algebra and system identification. Automatica **47**(9), 1896 – 1904 (2011). URL https://doi.org/10.1016/j.automatica.2011.06.013

[29] Ovchinnikov, A., Pogudin, G., Vo, T.: Bounds for elimination of unknowns in systems of differential-algebraic equations (2018). URL http://arxiv.org/abs/1610.04022. Preprint

[30] Pierce, D., Pillay, A.: A note on the axioms for differentially closed fields of characteristic zero. Journal of Algebra **204**(1), 108–115 (1998). URL http://dx.doi.org/10.1006/jabr.1997.7359

[31] Roeger, L., Allen, L.: Discrete May–Leonard competition models I. Journal of Difference Equations and Applications **10**(1), 77–98 (2004). URL http://dx.doi.org/10.1080/10236190310001603662

[32] Shafarevich, I.: Basic Algebraic Geometry 1. University Lecture Series. Springer (2013). URL http://dx.doi.org/10.1007/978-3-642-37956-7

[33] Stacks Project Authors, T.: *Stacks Project*. https://stacks.math.columbia.edu (2018)

[34] Stanley, R.P.: Enumerative Combinatorics: Volume 1, 2 edn. Cambridge University Press (2011)

[35] Stillman, M., Takayama, N., Verschelde, J.: Software for Algebraic Geometry. Springer (2008). URL http://dx.doi.org/10.1007/978-0-387-78133-4

[36] Tomašić, I.: Twisted Galois stratification. Nagoya Mathematical Journal **222**(1), 1–60 (2016). URL http://dx.doi.org/10.1017/nmj.2016.9

[37] Tomašić, I.: Direct twisted Galois stratification. Annals of Pure and Applied Logic **169**(1), 21–53 (2018). URL http://dx.doi.org/10.1016/j.apal.2017.07.002

[38] Varshavsky, Y.: Intersection of a correspondence with a graph of Frobenius. Journal of Algebraic Geometry **27**, 1–20 (2018). URL http://dx.doi.org/10.1090/jag/676

[39] Zippel, R.: Effective Polynomial Computation. Springer (1993). URL http://dx.doi.org/10.1007/978-1-4615-3188-3