Elimination and consistency checking for difference equations (even though the theory is undecidable!)

Thomas Scanlon [1]

UC Berkeley

14 September 2018

[1] This a report on joint work with Alexei Ovchinnikov and Gleb Pogudin available at `arXiv:1712.01412` and on on-going work with them and Wei Li.

The problem to be solved

Let us write $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_m)$ for these tuples of variables.

Given: Difference polynomials $f_1(\mathbf{x}; \mathbf{y}), \ldots, f_\ell(\mathbf{x}; \mathbf{y})$.

Determine: for which $\mathbf{b}$ the system $f_1(\mathbf{x}; \mathbf{b}) = \cdots = f_\ell(\mathbf{x}; \mathbf{b}) = 0$ is consistent.

- As an important special case, take $m = 0$ so that we are simply asking for a method to determine the consistency of a system of difference equations.
- In the version we solve, we work with a single distinguished endomorphism, so ordinary difference equations.
- By determine we mean that an algorithm is sought. Our goal is to produce a method which is, at least in principle, practically implementable.
- In the end, we address the weaker problem of producing a nontrivial difference equation satisfied by $\mathbf{b}$ if the solvability of the system implies that such must exist.

The problem to be solved

Let us write $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_m)$ for these tuples of variables.

Given: Difference polynomials $f_1(\mathbf{x}; \mathbf{y}), \ldots, f_\ell(\mathbf{x}; \mathbf{y})$.

Determine: for which $\mathbf{b}$ the system $f_1(\mathbf{x}; \mathbf{b}) = \cdots = f_\ell(\mathbf{x}; \mathbf{b}) = 0$ is consistent.

- As an important special case, take $m = 0$ so that we are simply asking for a method to determine the consistency of a system of difference equations.
- In the version we solve, we work with a single distinguished endomorphism, so ordinary difference equations.
- By determine we mean that an algorithm is sought. Our goal is to produce a method which is, at least in principle, practically implementable.
- In the end, we address the weaker problem of producing a nontrivial difference equation satisfied by $\mathbf{b}$ if the solvability of the system implies that such must exist.

The problem to be solved

Let us write $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_m)$ for these tuples of variables.

Given: Difference polynomials $f_1(\mathbf{x}; \mathbf{y}), \ldots, f_\ell(\mathbf{x}; \mathbf{y})$.

Determine: for which $\mathbf{b}$ the system $f_1(\mathbf{x}; \mathbf{b}) = \cdots = f_\ell(\mathbf{x}; \mathbf{b}) = 0$ is consistent.

- As an important special case, take $m = 0$ so that we are simply asking for a method to determine the consistency of a system of difference equations.
- In the version we solve, we work with a single distinguished endomorphism, so ordinary difference equations.
- By determine we mean that an algorithm is sought. Our goal is to produce a method which is, at least in principle, practically implementable.
- In the end, we address the weaker problem of producing a nontrivial difference equation satisfied by $\mathbf{b}$ if the solvability of the system implies that such must exist.

The problem to be solved

Let us write $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_m)$ for these tuples of variables.

Given: Difference polynomials $f_1(\mathbf{x}; \mathbf{y}), \ldots, f_\ell(\mathbf{x}; \mathbf{y})$.

Determine: for which $\mathbf{b}$ the system $f_1(\mathbf{x}; \mathbf{b}) = \cdots = f_\ell(\mathbf{x}; \mathbf{b}) = 0$ is consistent.

- As an important special case, take $m = 0$ so that we are simply asking for a method to determine the consistency of a system of difference equations.
- In the version we solve, we work with a single distinguished endomorphism, so ordinary difference equations.
- By determine we mean that an algorithm is sought. Our goal is to produce a method which is, at least in principle, practically implementable.
- In the end, we address the weaker problem of producing a nontrivial difference equation satisfied by $\mathbf{b}$ if the solvability of the system implies that such must exist.

The problem to be solved

Let us write $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_m)$ for these tuples of variables.

Given: Difference polynomials $f_1(\mathbf{x}; \mathbf{y}), \ldots, f_\ell(\mathbf{x}; \mathbf{y})$.

Determine: for which $\mathbf{b}$ the system $f_1(\mathbf{x}; \mathbf{b}) = \cdots = f_\ell(\mathbf{x}; \mathbf{b}) = 0$ is consistent.

- As an important special case, take $m = 0$ so that we are simply asking for a method to determine the consistency of a system of difference equations.
- In the version we solve, we work with a single distinguished endomorphism, so ordinary difference equations.
- By determine we mean that an algorithm is sought. Our goal is to produce a method which is, at least in principle, practically implementable.
- In the end, we address the weaker problem of producing a nontrivial difference equation satisfied by $\mathbf{b}$ if the solvability of the system implies that such must exist.

The problem to be solved

Let us write $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_m)$ for these tuples of variables.

Given: Difference polynomials $f_1(\mathbf{x}; \mathbf{y}), \ldots, f_\ell(\mathbf{x}; \mathbf{y})$.

Determine: for which $\mathbf{b}$ the system $f_1(\mathbf{x}; \mathbf{b}) = \cdots = f_\ell(\mathbf{x}; \mathbf{b}) = 0$ is consistent.

- As an important special case, take $m = 0$ so that we are simply asking for a method to determine the consistency of a system of difference equations.
- In the version we solve, we work with a single distinguished endomorphism, so ordinary difference equations.
- By determine we mean that an algorithm is sought. Our goal is to produce a method which is, at least in principle, practically implementable.
- In the end, we address the weaker problem of producing a nontrivial difference equation satisfied by $\mathbf{b}$ if the solvability of the system implies that such must exist.

Some difference algebra

Difference equations (on functions) are usually expressed by asserting that some equation holds between the function and some transforms of the function by shifting the arguments.

For example, the Γ function satisfies the difference equation $\Gamma(x+1) = x\Gamma(x)$.

We algebraize this by working with difference rings, (R, σ), a commutative rings R given together with a distinguished ring endomorphism $\sigma : R \to R$.

We treat difference rings as structures in the language of difference rings, $\mathscr{L}(+, \cdot, -, 0, 1, \sigma)$, and modulo the theory of difference rings, terms in this language may be identified with difference polynomials, expressions of the form $P(\mathbf{x}, \sigma\mathbf{x}, \ldots, \sigma^d(\mathbf{x}))$ where P is an ordinary polynomial.

Allow ourselves parameters from R, the difference polynomials with coefficients from R in the variables $x_1, \ldots, x_n$ form a difference ring $R\{x_1, \ldots, x_n\}_\sigma$. If we also allow σ^{-1} as a function symbol, we have the inversive difference polynomials $R\{x_1, \ldots, x_n\}_{\sigma,\sigma^{-1}}$.

Some difference algebra

Difference equations (on functions) are usually expressed by asserting that some equation holds between the function and some transforms of the function by shifting the arguments.

For example, the Γ function satisfies the difference equation $\Gamma(x+1) = x\Gamma(x)$.

We algebraize this by working with difference rings, (R, σ), a commutative rings R given together with a distinguished ring endomorphism $\sigma : R \to R$.

We treat difference rings as structures in the language of difference rings, $\mathscr{L}(+, \cdot, -, 0, 1, \sigma)$, and modulo the theory of difference rings, terms in this language may be identified with difference polynomials, expressions of the form $P(\mathbf{x}, \sigma\mathbf{x}, \ldots, \sigma^d(\mathbf{x}))$ where P is an ordinary polynomial.

Allow ourselves parameters from R, the difference polynomials with coefficients from R in the variables $x_1, \ldots, x_n$ form a difference ring $R\{x_1, \ldots, x_n\}_\sigma$. If we also allow σ^{-1} as a function symbol, we have the inversive difference polynomials $R\{x_1, \ldots, x_n\}_{\sigma,\sigma^{-1}}$.

Some difference algebra

Difference equations (on functions) are usually expressed by asserting that some equation holds between the function and some transforms of the function by shifting the arguments.

For example, the Γ function satisfies the difference equation $\Gamma(x+1) = x\Gamma(x)$.

We algebraize this by working with difference rings, (R, σ), a commutative rings R given together with a distinguished ring endomorphism $\sigma : R \to R$.

We treat difference rings as structures in the language of difference rings, $\mathscr{L}(+, \cdot, -, 0, 1, \sigma)$, and modulo the theory of difference rings, terms in this language may be identified with difference polynomials, expressions of the form $P(\mathbf{x}, \sigma\mathbf{x}, \ldots, \sigma^d(\mathbf{x}))$ where P is an ordinary polynomial.

Allow ourselves parameters from R, the difference polynomials with coefficients from R in the variables $x_1, \ldots, x_n$ form a difference ring $R\{x_1, \ldots, x_n\}_\sigma$. If we also allow σ^{-1} as a function symbol, we have the inversive difference polynomials $R\{x_1, \ldots, x_n\}_{\sigma,\sigma^{-1}}$.

Some difference algebra

Difference equations (on functions) are usually expressed by asserting that some equation holds between the function and some transforms of the function by shifting the arguments.

For example, the Γ function satisfies the difference equation $\Gamma(x+1) = x\Gamma(x)$.

We algebraize this by working with difference rings, (R, σ), a commutative rings R given together with a distinguished ring endomorphism $\sigma : R \to R$.

We treat difference rings as structures in the language of difference rings, $\mathscr{L}(+, \cdot, -, 0, 1, \sigma)$, and modulo the theory of difference rings, terms in this language may be identified with difference polynomials, expressions of the form $P(\mathbf{x}, \sigma\mathbf{x}, \ldots, \sigma^d(\mathbf{x}))$ where P is an ordinary polynomial.

Allow ourselves parameters from R, the difference polynomials with coefficients from R in the variables $x_1, \ldots, x_n$ form a difference ring $R\{x_1, \ldots, x_n\}_\sigma$. If we also allow σ^{-1} as a function symbol, we have the inversive difference polynomials $R\{x_1, \ldots, x_n\}_{\sigma,\sigma^{-1}}$.

Some difference algebra

Difference equations (on functions) are usually expressed by asserting that some equation holds between the function and some transforms of the function by shifting the arguments.

For example, the Γ function satisfies the difference equation $\Gamma(x+1) = x\Gamma(x)$.

We algebraize this by working with difference rings, (R, σ), a commutative rings R given together with a distinguished ring endomorphism $\sigma : R \to R$.

We treat difference rings as structures in the language of difference rings, $\mathscr{L}(+, \cdot, -, 0, 1, \sigma)$, and modulo the theory of difference rings, terms in this language may be identified with difference polynomials, expressions of the form $P(\mathbf{x}, \sigma\mathbf{x}, \ldots, \sigma^d(\mathbf{x}))$ where P is an ordinary polynomial.

Allow ourselves parameters from R, the difference polynomials with coefficients from R in the variables $x_1, \ldots, x_n$ form a difference ring $R\{x_1, \ldots, x_n\}_\sigma$. If we also allow σ^{-1} as a function symbol, we have the inversive difference polynomials $R\{x_1, \ldots, x_n\}_{\sigma,\sigma^{-1}}$.

Solving the problem in difference fields

If consistent means "has a solution in some difference field extension", then the known work around ACFA (essentially) solves the problem (though improvements may be possible through better results in computational difference algebra).

- ACFA, the model companion of the theory of difference fields, is not complete, but its completions are understood. Thus, on general grounds, the consistency problem is decidable.
- Related to this point, since ACFA does not admit quantifier elimination in the language of difference rings, the formula $\exists x \bigwedge f_i(x, y) = 0$ is not equivalent to a quantifier-free formula in general, but the near quantifier elimination of [Chatzidakis-Hrushovski, *JLMS*, 1999] or the Galois stratification formalism of [Tomasič, *Nagoya*, 2016] the problem of describing the parameters for which the equations are consistent may be resolved.
- More importantly, from the geometric axiomatization of ACFA one may produce algorithms to resolve these problems.

Solving the problem in difference fields

If consistent means "has a solution in some difference field extension", then the known work around ACFA (essentially) solves the problem (though improvements may be possible through better results in computational difference algebra).

- ACFA, the model companion of the theory of difference fields, is not complete, but its completions are understood. Thus, on general grounds, the consistency problem is decidable.
- Related to this point, since ACFA does not admit quantifier elimination in the language of difference rings, the formula $\exists x \bigwedge f_i(x, y) = 0$ is not equivalent to a quantifier-free formula in general, but the near quantifier elimination of [Chatzidakis-Hrushovski, *JLMS*, 1999] or the Galois stratification formalism of [Tomasič, *Nagoya*, 2016] the problem of describing the parameters for which the equations are consistent may be resolved.
- More importantly, from the geometric axiomatization of ACFA one may produce algorithms to resolve these problems.

Solving the problem in difference fields

If consistent means "has a solution in some difference field extension", then the known work around ACFA (essentially) solves the problem (though improvements may be possible through better results in computational difference algebra).

- ACFA, the model companion of the theory of difference fields, is not complete, but its completions are understood. Thus, on general grounds, the consistency problem is decidable.
- Related to this point, since ACFA does not admit quantifier elimination in the language of difference rings, the formula $\exists \mathbf{x} \bigwedge f_i(\mathbf{x}, \mathbf{y}) = 0$ is not equivalent to a quantifier-free formula in general, but the near quantifier elimination of [Chatzidakis-Hrushovski, *JLMS*, 1999] or the Galois stratification formalism of [Tomasič, *Nagoya*, 2016] the problem of describing the parameters for which the equations are consistent may be resolved.
- More importantly, from the geometric axiomatization of ACFA one may produce algorithms to resolve these problems.

Geometric axioms

Recall the geometric axiomatization of ACFA.

A difference field (K, σ) is a model of ACFA if and only if

- K is algebraically closed
- $\sigma : K \to K$ is an automorphism
- For any irreducible affine algebraic variety V and $W \subseteq V \times V^\sigma$ a closed subvariety for which both projections $W \to V$ and $W \to V^\sigma$ are dominant, then there is a point $a \in V(K)$ with $(a, \sigma(a)) \in W(K)$.

Geometric axioms

Recall the geometric axiomatization of ACFA.
A difference field (K, σ) is a model of ACFA if and only if

- K is algebraically closed
- $\sigma : K \to K$ is an automorphism
- For any irreducible affine algebraic variety V and $W \subseteq V \times V^\sigma$ a closed subvariety for which both projections $W \to V$ and $W \to V^\sigma$ are dominant, then there is a point $\mathbf{a} \in V(K)$ with $(\mathbf{a}, \sigma(\mathbf{a})) \in W(K)$.

Geometric axioms

Recall the geometric axiomatization of ACFA.
A difference field (K, σ) is a model of ACFA if and only if

- K is algebraically closed
- $\sigma : K \to K$ is an automorphism
- For any irreducible affine algebraic variety V and $W \subseteq V \times V^\sigma$ a closed subvariety for which both projections $W \to V$ and $W \to V^\sigma$ are dominant, then there is a point $\mathbf{a} \in V(K)$ with $(\mathbf{a}, \sigma(\mathbf{a})) \in W(K)$.

Geometric axioms

Recall the geometric axiomatization of ACFA.
A difference field (K, σ) is a model of ACFA if and only if

- K is algebraically closed
- $\sigma : K \to K$ is an automorphism
- For any irreducible affine algebraic variety V and $W \subseteq V \times V^\sigma$ a closed subvariety for which both projections $W \to V$ and $W \to V^\sigma$ are dominant, then there is a point $\mathbf{a} \in V(K)$ with $(\mathbf{a}, \sigma(\mathbf{a})) \in W(K)$.

Geometric axioms

Recall the geometric axiomatization of ACFA.
A difference field (K, σ) is a model of ACFA if and only if

- K is algebraically closed
- $\sigma : K \to K$ is an automorphism
- For any irreducible affine algebraic variety V and $W \subseteq V \times V^\sigma$ a closed subvariety for which both projections $W \to V$ and $W \to V^\sigma$ are dominant, then there is a point $\mathbf{a} \in V(K)$ with $(\mathbf{a}, \sigma(\mathbf{a})) \in W(K)$.

A little algebraic geometry for the geometric axioms

We give the requisite definitions in terms of rational points in affine space; those of you who are familiar with other formalisms for algebraic geometry know how to adjust the statements appropriately.

Let K be an algebraically closed field.

- By an algebraic variety X we will mean a subset of K^n (for some n) defined by the vanishing of some finite system of polynomial equations.
- X is irreducible if it cannot be expressed as the union of two proper subvarieties.
- If $X \subseteq K^{n+m}$ and $Y \subseteq K^n$ are irreducible varieties, then we say that projection $\pi : K^{n+m} \to K^n$ gives a dominant map from X to Y if $\pi(X) \subseteq Y$ and $Y \setminus \pi(X)$ is contained in proper subvariety of Y.
- Quantifier elimination for the theory of algebraically closed fields implies that the image of an algebraic variety under coordinate projections is finite Boolean combination of algebraic varieties.
- It is a nontrivial theorem that irreducibility and dominance of a projection are definable uniformly in parameters.

A little algebraic geometry for the geometric axioms

We give the requisite definitions in terms of rational points in affine space; those of you who are familiar with other formalisms for algebraic geometry know how to adjust the statements appropriately.
Let K be an algebraically closed field.

- By an algebraic variety X we will mean a subset of K^n (for some n) defined by the vanishing of some finite system of polynomial equations.
- X is irreducible if it cannot be expressed as the union of two proper subvarieties.
- If $X \subseteq K^{n+m}$ and $Y \subseteq K^n$ are irreducible varieties, then we say that projection $\pi : K^{n+m} \to K^n$ gives a dominant map from X to Y if $\pi(X) \subseteq Y$ and $Y \setminus \pi(X)$ is contained in proper subvariety of Y.
- Quantifier elimination for the theory of algebraically closed fields implies that the image of an algebraic variety under coordinate projections is finite Boolean combination of algebraic varieties.
- It is a nontrivial theorem that irreducibility and dominance of a projection are definable uniformly in parameters.

A little algebraic geometry for the geometric axioms

We give the requisite definitions in terms of rational points in affine space; those of you who are familiar with other formalisms for algebraic geometry know how to adjust the statements appropriately.

Let K be an algebraically closed field.

- By an algebraic variety X we will mean a subset of K^n (for some n) defined by the vanishing of some finite system of polynomial equations.
- X is irreducible if it cannot be expressed as the union of two proper subvarieties.
- If $X \subseteq K^{n+m}$ and $Y \subseteq K^n$ are irreducible varieties, then we say that projection $\pi : K^{n+m} \to K^n$ gives a dominant map from X to Y if $\pi(X) \subseteq Y$ and $Y \setminus \pi(X)$ is contained in proper subvariety of Y.
- Quantifier elimination for the theory of algebraically closed fields implies that the image of an algebraic variety under coordinate projections is finite Boolean combination of algebraic varieties.
- It is a nontrivial theorem that irreducibility and dominance of a projection are definable uniformly in parameters.

A little algebraic geometry for the geometric axioms

We give the requisite definitions in terms of rational points in affine space; those of you who are familiar with other formalisms for algebraic geometry know how to adjust the statements appropriately.

Let K be an algebraically closed field.

- By an algebraic variety X we will mean a subset of K^n (for some n) defined by the vanishing of some finite system of polynomial equations.
- X is irreducible if it cannot be expressed as the union of two proper subvarieties.
- If $X \subseteq K^{n+m}$ and $Y \subseteq K^n$ are irreducible varieties, then we say that projection $\pi : K^{n+m} \to K^n$ gives a dominant map from X to Y if $\pi(X) \subseteq Y$ and $Y \setminus \pi(X)$ is contained in proper subvariety of Y.
- Quantifier elimination for the theory of algebraically closed fields implies that the image of an algebraic variety under coordinate projections is finite Boolean combination of algebraic varieties.
- It is a nontrivial theorem that irreducibility and dominance of a projection are definable uniformly in parameters.

A little algebraic geometry for the geometric axioms

We give the requisite definitions in terms of rational points in affine space; those of you who are familiar with other formalisms for algebraic geometry know how to adjust the statements appropriately.

Let K be an algebraically closed field.

- By an algebraic variety X we will mean a subset of K^n (for some n) defined by the vanishing of some finite system of polynomial equations.
- X is irreducible if it cannot be expressed as the union of two proper subvarieties.
- If $X \subseteq K^{n+m}$ and $Y \subseteq K^n$ are irreducible varieties, then we say that projection $\pi : K^{n+m} \to K^n$ gives a dominant map from X to Y if $\pi(X) \subseteq Y$ and $Y \setminus \pi(X)$ is contained in proper subvariety of Y.
- Quantifier elimination for the theory of algebraically closed fields implies that the image of an algebraic variety under coordinate projections is finite Boolean combination of algebraic varieties.
- It is a nontrivial theorem that irreducibility and dominance of a projection are definable uniformly in parameters.

A little algebraic geometry for the geometric axioms

We give the requisite definitions in terms of rational points in affine space; those of you who are familiar with other formalisms for algebraic geometry know how to adjust the statements appropriately.

Let K be an algebraically closed field.

- By an algebraic variety X we will mean a subset of K^n (for some n) defined by the vanishing of some finite system of polynomial equations.
- X is irreducible if it cannot be expressed as the union of two proper subvarieties.
- If $X \subseteq K^{n+m}$ and $Y \subseteq K^n$ are irreducible varieties, then we say that projection $\pi : K^{n+m} \to K^n$ gives a dominant map from X to Y if $\pi(X) \subseteq Y$ and $Y \setminus \pi(X)$ is contained in proper subvariety of Y.
- Quantifier elimination for the theory of algebraically closed fields implies that the image of an algebraic variety under coordinate projections is finite Boolean combination of algebraic varieties.
- It is a nontrivial theorem that irreducibility and dominance of a projection are definable uniformly in parameters.

A little algebraic geometry for the geometric axioms

We give the requisite definitions in terms of rational points in affine space; those of you who are familiar with other formalisms for algebraic geometry know how to adjust the statements appropriately.

Let K be an algebraically closed field.

- By an algebraic variety X we will mean a subset of K^n (for some n) defined by the vanishing of some finite system of polynomial equations.
- X is irreducible if it cannot be expressed as the union of two proper subvarieties.
- If $X \subseteq K^{n+m}$ and $Y \subseteq K^n$ are irreducible varieties, then we say that projection $\pi : K^{n+m} \to K^n$ gives a dominant map from X to Y if $\pi(X) \subseteq Y$ and $Y \setminus \pi(X)$ is contained in proper subvariety of Y.
- Quantifier elimination for the theory of algebraically closed fields implies that the image of an algebraic variety under coordinate projections is finite Boolean combination of algebraic varieties.
- It is a nontrivial theorem that irreducibility and dominance of a projection are definable uniformly in parameters.

Prolongation-Projection method (also called the Decomposition-Elimination-Prolongation [DEP] method) – Step 0

We are given difference polynomials $f_1(\mathbf{x}), \ldots, f_\ell(\mathbf{x})$ and wish to determine whether it is consistent that there be a solution in a difference field.

Step 0 (convert to order one): If, for example, $f_i(\mathbf{x}) = F_i(\mathbf{x}, \sigma(\mathbf{x}), \ldots, \sigma^k(\mathbf{x}))$ where F_i is an ordinary polynomial, we add new variables $x_{i,j}$ for $1 \leq i \leq n$ and $0 \leq j < k$, and work with the new equations $F_i(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \sigma(\mathbf{x}_{k-1})) = 0$ and $\sigma(\mathbf{x}_j) = \mathbf{x}_{j+1}$ for $0 \leq j < k - 1$. From now on, we assume that each equation takes the form $f_i(\mathbf{x}) = F_i(\mathbf{x}, \sigma(\mathbf{x})) = 0$ where F_i is an ordinary polynomial.

Prolongation-Projection method (also called the Decomposition-Elimination-Prolongation [DEP] method) – Step 0

We are given difference polynomials $f_1(\mathbf{x}), \ldots, f_\ell(\mathbf{x})$ and wish to determine whether it is consistent that there be a solution in a difference field.

Step 0 (convert to order one): If, for example, $f_i(\mathbf{x}) = F_i(\mathbf{x}, \sigma(\mathbf{x}), \ldots, \sigma^k(\mathbf{x}))$ where F_i is an ordinary polynomial, we add new variables $x_{i,j}$ for $1 \leq i \leq n$ and $0 \leq j < k$, and work with the new equations $F_i(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \sigma(\mathbf{x}_{k-1})) = 0$ and $\sigma(\mathbf{x}_j) = \mathbf{x}_{j+1}$ for $0 \leq j < k-1$. From now on, we assume that each equation takes the form $f_i(\mathbf{x}) = F_i(\mathbf{x}, \sigma(\mathbf{x})) = 0$ where F_i is an ordinary polynomial.

DEP – main steps

- Consider the algebraic variety W defined by $F_1(\mathrm{x}, \mathrm{x}') = \cdots = F_\ell(\mathrm{x}, \mathrm{x}') = 0$. Decompose W into its irreducible components $W = \bigcup W_i$. There is a solution to our problem if and only if for some i we can find $\mathbf{a}$ with $(\mathbf{a}, \sigma(\mathbf{a})) \in W_i(K)$. We thus reduce to the case that W is irreducible.
- By quantifier elimination in ACF, we may compute V, the projection of W to the x-space. Likewise, we may compute V', the projection of W to the x'-space.
- We consider the prolongation space $V \times V^\sigma$. If $V' = V^\sigma$ and $W \subseteq V \times V^\sigma$, then from the geometric axioms we have a solution. Otherwise, replace W with $W \cap ((V')^{\sigma^{-1}} \times V^\sigma)$ and repeat.

DEP – main steps

- Consider the algebraic variety W defined by $F_1(\mathbf{x}, \mathbf{x}') = \cdots = F_\ell(\mathbf{x}, \mathbf{x}') = 0$. Decompose W into its irreducible components $W = \bigcup W_i$. There is a solution to our problem if and only if for some i we can find $\mathbf{a}$ with $(\mathbf{a}, \sigma(\mathbf{a})) \in W_i(K)$. We thus reduce to the case that W is irreducible.
- By quantifier elimination in ACF, we may compute V, the projection of W to the $\mathbf{x}$-space. Likewise, we may compute V', the projection of W to the $\mathbf{x}'$-space.
- We consider the prolongation space $V \times V^\sigma$. If $V' = V^\sigma$ and $W \subseteq V \times V^\sigma$, then from the geometric axioms we have a solution. Otherwise, replace W with $W \cap ((V')^{\sigma^{-1}} \times V^\sigma)$ and repeat.

DEP – main steps

- Consider the algebraic variety W defined by $F_1(\mathbf{x},\mathbf{x}') = \cdots = F_\ell(\mathbf{x},\mathbf{x}') = 0$. Decompose W into its irreducible components $W = \bigcup W_i$. There is a solution to our problem if and only if for some i we can find $\mathbf{a}$ with $(\mathbf{a},\sigma(\mathbf{a})) \in W_i(K)$. We thus reduce to the case that W is irreducible.
- By quantifier elimination in ACF, we may compute V, the projection of W to the $\mathbf{x}$-space. Likewise, we may compute V', the projection of W to the $\mathbf{x}'$-space.
- We consider the prolongation space $V \times V^\sigma$. If $V' = V^\sigma$ and $W \subseteq V \times V^\sigma$, then from the geometric axioms we have a solution. Otherwise, replace W with $W \cap ((V')^{\sigma^{-1}} \times V^\sigma)$ and repeat.

DEP – history and complexity

- DEP for algebraic difference equations is introduced to prove explicit bounds for the Manin-Mumford conjecture in [Hrushovski, *APAL*, 2001]. An analogous technique for differential equations is used in [Hrushovski-Pillay, *IMRN*, 2000] to prove explicit bounds in the function field Mordell-Lang conjecture.
- The number of steps in the procedure outlined grows doubly exponentially in the dimension of the initial W. A more streamlined approach (presented in the differential setting) avoiding some of the implicit recursion with singly exponential bounds may be found in [Binyamini, *Compositio*, 2017].

DEP – history and complexity

- DEP for algebraic difference equations is introduced to prove explicit bounds for the Manin-Mumford conjecture in [Hrushovski, *APAL*, 2001]. An analogous technique for differential equations is used in [Hrushovski-Pillay, *IMRN*, 2000] to prove explicit bounds in the function field Mordell-Lang conjecture.
- The number of steps in the procedure outlined grows doubly exponentially in the dimension of the initial W. A more streamlined approach (presented in the differential setting) avoiding some of the implicit recursion with singly exponential bounds may be found in [Binyamini, *Compositio*, 2017].

Solving difference equations in sequence rings

In practice, solutions to difference equations are sought in sequences.

If R is any ring, then $R^{\mathbb{N}}$ and $R^{\mathbb{Z}}$ are difference rings with the distinguished endomorphism taken to be the shift operator $\sigma : (a_n) \mapsto (a_{n+1})$. Neither of these difference rings embeds into a difference field.

Moreover, there are natural systems of difference equations which are inconsistent relative to the theory of difference fields but which may be solved in sequences. For example, the sequence $(0, 1, 0, 1, 0, 1, \ldots)$ is a solution to the system $x\sigma(x) = 0$ and $x + \sigma(x) = 1$.

Solving difference equations in sequence rings

In practice, solutions to difference equations are sought in sequences.

If R is any ring, then $R^{\mathbb{N}}$ and $R^{\mathbb{Z}}$ are difference rings with the distinguished endomorphism taken to be the shift operator $\sigma : (a_n) \mapsto (a_{n+1})$. Neither of these difference rings embeds into a difference field.

Moreover, there are natural systems of difference equations which are inconsistent relative to the theory of difference fields but which may be solved in sequences. For example, the sequence $(0, 1, 0, 1, 0, 1, \ldots)$ is a solution to the system $x\sigma(x) = 0$ and $x + \sigma(x) = 1$.

Solving difference equations in sequence rings

In practice, solutions to difference equations are sought in sequences.

If R is any ring, then $R^{\mathbb{N}}$ and $R^{\mathbb{Z}}$ are difference rings with the distinguished endomorphism taken to be the shift operator $\sigma : (a_n) \mapsto (a_{n+1})$. Neither of these difference rings embeds into a difference field.

Moreover, there are natural systems of difference equations which are inconsistent relative to the theory of difference fields but which may be solved in sequences. For example, the sequence $(0, 1, 0, 1, 0, 1, \ldots)$ is a solution to the system $x\sigma(x) = 0$ and $x + \sigma(x) = 1$.

A model companion for difference rings?

We might try to emulate the solution to the problem for difference fields by finding a model companion to the theory of difference rings (or, perhaps, reduced commutative difference rings). However, it is shown in [Hrushovski-Point, *J. Algebra*, 2007] that sequence rings $K^{\mathbb{N}}$ and $K^{\mathbb{Z}}$ with K infinite, and, indeed, all commutative von Neumann regular $[(\forall x)(\exists z) x = x^2 z]$ difference rings have undecidable theories.

For K a field of characteristic zero, if $R = K^{\mathbb{N}}$ or $K^{\mathbb{Z}}$, then $\mathbb{Z} \subseteq R$ is defined by $x \in \mathbb{Z} \Longleftrightarrow$

- $\sigma(x) = x$ and
- $(\exists y)[\sigma(y) = y + 1$
- & y is not a unit
- & $(y - x)$ is not a unit]

A model companion for difference rings?

We might try to emulate the solution to the problem for difference fields by finding a model companion to the theory of difference rings (or, perhaps, reduced commutative difference rings). However, it is shown in [Hrushovski-Point, *J. Algebra*, 2007] that sequence rings $K^{\mathbb{N}}$ and $K^{\mathbb{Z}}$ with K infinite, and, indeed, all commutative von Neumann regular $[(\forall x)(\exists z) x = x^2 z]$ difference rings have undecidable theories.

For K a field of characteristic zero, if $R = K^{\mathbb{N}}$ or $K^{\mathbb{Z}}$, then $\mathbb{Z} \subseteq R$ is defined by $x \in \mathbb{Z} \Longleftrightarrow$

- $\sigma(x) = x$ and
- $(\exists y)[\sigma(y) = y + 1$
- & y is not a unit
- & $(y - x)$ is not a unit]

An abstract difference Nullstellensatz

Despite the undecidability of sequence rings as difference rings, it is not hard to establish an abstract Nullstellensatz for difference equations.

An abstract difference Nullstellensatz

Despite the undecidability of sequence rings as difference rings, it is not hard to establish an abstract Nullstellensatz for difference equations.

Proposition

For all uncountable algebraically closed fields K and finite sets $S \subseteq K\{x_1, \ldots, x_n\}_\sigma$, the following statements are equivalent:

1. *S has a solution in $K^{\mathbb{Z}}$.*
2. *S has a solution in $K^{\mathbb{N}}$.*
3. *S has finite partial solutions of length ℓ for all $\ell \gg 0$.*
4. *The ideal $[S] := (\{\sigma^j(P) \mid P \in S, j \in \mathbb{N}\}) \subseteq K\{x_1, \ldots, x_n\}_\sigma$ does not contain 1.*
5. *The ideal $[S]^* := (\{\sigma^j(P) \mid P \in S, j \in \mathbb{Z}\}) \subseteq K\{x_1, \ldots, x_n\}_{\sigma,\sigma^{-1}}$ does not contain 1.*
6. *S has a solution in some difference K-algebra.*

An abstract difference Nullstellensatz

Despite the undecidability of sequence rings as difference rings, it is not hard to establish an abstract Nullstellensatz for difference equations.

Proposition

For all uncountable *algebraically closed fields K and finite sets $S \subseteq K\{x_1, \ldots, x_n\}_\sigma$, the following statements are equivalent:*

1. *S has a solution in $K^{\mathbb{Z}}$.*
2. *S has a solution in $K^{\mathbb{N}}$.*
3. *S has finite partial solutions of length ℓ for all $\ell \gg 0$.*
4. *The ideal $[S] := (\{\sigma^j(P) \mid P \in S, j \in \mathbb{N}\}) \subseteq K\{x_1, \ldots, x_n\}_\sigma$ does not contain 1.*
5. *The ideal $[S]^* := (\{\sigma^j(P) \mid P \in S, j \in \mathbb{Z}\}) \subseteq K\{x_1, \ldots, x_n\}_{\sigma,\sigma^{-1}}$ does not contain 1.*
6. *S has a solution in some difference K-algebra.*

About the proof – where is uncountability used?

The only difficult step is to show 6. (S has a solution in some difference K-algebra) implies 1. (S has a solution in $K^{\mathbb{Z}}$).

This is really done by noting that 6. and 5. ($1 \notin [S]^*$) are easily equivalent, taking $\mathfrak{m} \supseteq [S]^*$ a maximal ideal (but not necessarily a difference ideal!) containing $[S]^*$, and constructing a sequence solution from $K\{x_1, \ldots, x_n\}_{\sigma,\sigma^{-1}}/\mathfrak{m}$. One uses $\aleph_1$-saturation of K to show that this sequence may be realized by a sequence from K.

Question: Is uncountability an essential hypothesis?

About the proof – where is uncountability used?

The only difficult step is to show 6. (S has a solution in some difference K-algebra) implies 1. (S has a solution in $K^{\mathbb{Z}}$).

This is really done by noting that 6. and 5. ($1 \notin [S]^*$) are easily equivalent, taking $\mathfrak{m} \supseteq [S]^*$ a maximal ideal (but not necessarily a difference ideal!) containing $[S]^*$, and constructing a sequence solution from $K\{x_1, \ldots, x_n\}_{\sigma,\sigma^{-1}}/\mathfrak{m}$. One uses $\aleph_1$-saturation of K to show that this sequence may be realized by a sequence from K.

Question: Is uncountability an essential hypothesis?

About the proof – where is uncountability used?

The only difficult step is to show 6. (S has a solution in some difference K-algebra) implies 1. (S has a solution in $K^{\mathbb{Z}}$).

This is really done by noting that 6. and 5. ($1 \notin [S]^*$) are easily equivalent, taking $\mathfrak{m} \supseteq [S]^*$ a maximal ideal (but not necessarily a difference ideal!) containing $[S]^*$, and constructing a sequence solution from $K\{x_1, \ldots, x_n\}_{\sigma,\sigma^{-1}}/\mathfrak{m}$. One uses $\aleph_1$-saturation of K to show that this sequence may be realized by a sequence from K.

Question: Is uncountability an essential hypothesis?

Reducing to an algebraic problem

For R a difference ring and $S \subseteq R\{x_1, \ldots, x_n\}_\sigma$, let $h := \min\{r \in \mathbb{N} \ : \ S \subseteq R[\sigma^j(x_i) \ : \ 0 \leq j \leq r, 1 \leq i \leq n\}$ be the order of S. For $N \in \mathbb{N}$, we set $[S]_N := (\{\sigma^j(s) \ : \ s \in S, 0 \leq j \leq N\}) \subseteq R[\mathbf{x}, \sigma(\mathbf{x}), \ldots, \sigma^{h+r}(\mathbf{x})]$.

From the difference Nullstellensatz, we see that inconsistency of a system $S \subseteq K\{\mathbf{x}\}_\sigma$ of difference equations is equivalent to the existence of some $N \in \mathbb{N}$ with $1 \in [S]_N$. If we knew a bound on N, then eventual consistency would be axiomatizable and checking this condition would reduce to a standard ideal membership problem in a polynomial ring.

Reducing to an algebraic problem

For R a difference ring and $S \subseteq R\{x_1, \ldots, x_n\}_\sigma$, let $h := \min\{r \in \mathbb{N} \ : \ S \subseteq R[\sigma^j(x_i) \ : \ 0 \leq j \leq r, 1 \leq i \leq n\}$ be the order of S. For $N \in \mathbb{N}$, we set $[S]_N := (\{\sigma^j(s) \ : \ s \in S, 0 \leq j \leq N\}) \subseteq R[\mathbf{x}, \sigma(\mathbf{x}), \ldots, \sigma^{h+r}(\mathbf{x})]$.

From the difference Nullstellensatz, we see that inconsistency of a system $S \subseteq K\{\mathbf{x}\}_\sigma$ of difference equations is equivalent to the existence of some $N \in \mathbb{N}$ with $1 \in [S]_N$. If we knew a bound on N, then eventual consistency would be axiomatizable and checking this condition would reduce to a standard ideal membership problem in a polynomial ring.

Elimination

Let R be any commutative ring and $S \subseteq R[\mathbf{x};\mathbf{y}]$ a set of polynomials in the variables $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_m)$. By the elimination ideal of S we mean $(S) \cap R[\mathbf{y}]$.

Likewise, for R difference ring and $S \subseteq R\{\mathbf{x};\mathbf{y}\}_\sigma$ a set of difference polynomials. The difference elimination ideal of S is $R\{\mathbf{y}\}_\sigma \cap [S]$.

The difference elimination ideal of S describes the Cohn closure of the set defined by $\exists \mathbf{y} \bigwedge_{f \in S} f(\mathbf{x}, \mathbf{y}) = 0$.

Elimination

Let R be any commutative ring and $S \subseteq R[\mathbf{x}; \mathbf{y}]$ a set of polynomials in the variables $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_m)$. By the elimination ideal of S we mean $(S) \cap R[\mathbf{y}]$.

Likewise, for R difference ring and $S \subseteq R\{\mathbf{x}; \mathbf{y}\}_\sigma$ a set of difference polynomials. The difference elimination ideal of S is $R\{\mathbf{y}\}_\sigma \cap [S]$.

The difference elimination ideal of S describes the Cohn closure of the set defined by $\exists \mathbf{y} \bigwedge_{f \in S} f(\mathbf{x}, \mathbf{y}) = 0$.

Elimination

Let R be any commutative ring and $S \subseteq R[\mathbf{x}; \mathbf{y}]$ a set of polynomials in the variables $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_m)$. By the elimination ideal of S we mean $(S) \cap R[\mathbf{y}]$.

Likewise, for R difference ring and $S \subseteq R\{\mathbf{x}; \mathbf{y}\}_\sigma$ a set of difference polynomials. The difference elimination ideal of S is $R\{\mathbf{y}\}_\sigma \cap [S]$.

The difference elimination ideal of S describes the Cohn closure of the set defined by $\exists \mathbf{y} \bigwedge_{f \in S} f(\mathbf{x}, \mathbf{y}) = 0$.

Main theorem

Theorem

There is an explicitly computable function B of the complexity of finite sets of difference equations (e.g. number of variables, orders, total degrees, number of equations) so that for any difference field K and set $S \subseteq K\{\mathbf{x}, \mathbf{y}\}_\sigma$ of difference equations, so that if the difference elimination ideal of S is nontrivial, then so is the elimination ideal of $[S]_B$.

- When $m = 0$ (*i.e.*, when there are no y variables), by the Nullstellensatz, this gives a first-order condition for the existence of solutions to S in some sequence ring $L^{\mathbb{N}}$ with $L = L^{\mathrm{alg}}$ extending K and uncountable.
- The function B grows very quickly for underdetermined systems, but for practical elimination problems it tends to produce very small numbers.
- To ease notation, I will focus on the case where $m = 0$, but we should remember that for the applied parameter identification problems, the main point is to allow m to be large but the equations in x should be

Main theorem

Theorem

There is an explicitly computable function B of the complexity of finite sets of difference equations (e.g. number of variables, orders, total degrees, number of equations) so that for any difference field K and set $S \subseteq K\{\mathbf{x}, \mathbf{y}\}_\sigma$ of difference equations, so that if the difference elimination ideal of S is nontrivial, then so is the elimination ideal of $[S]_B$.

- When $m = 0$ (*i.e.*, when there are no $\mathbf{y}$ variables), by the Nullstellensatz, this gives a first-order condition for the existence of solutions to S in some sequence ring $L^{\mathbb{N}}$ with $L = L^{\text{alg}}$ extending K and uncountable.
- The function B grows very quickly for underdetermined systems, but for practical elimination problems it tends to produce very small numbers.
- To ease notation, I will focus on the case where $m = 0$, but we should remember that for the applied parameter identification problems, the main point is to allow m to be large but the equations in $\mathbf{x}$ should be

Main theorem

Theorem

There is an explicitly computable function B of the complexity of finite sets of difference equations (e.g. number of variables, orders, total degrees, number of equations) so that for any difference field K and set $S \subseteq K\{\mathbf{x}, \mathbf{y}\}_\sigma$ of difference equations, so that if the difference elimination ideal of S is nontrivial, then so is the elimination ideal of $[S]_B$.

- When $m = 0$ (*i.e.*, when there are no $\mathbf{y}$ variables), by the Nullstellensatz, this gives a first-order condition for the existence of solutions to S in some sequence ring $L^{\mathbb{N}}$ with $L = L^{\text{alg}}$ extending K and uncountable.
- The function B grows very quickly for underdetermined systems, but for practical elimination problems it tends to produce very small numbers.
- To ease notation, I will focus on the case where $m = 0$, but we should remember that for the applied parameter identification problems, the main point is to allow m to be large but the equations in $\mathbf{x}$ should be

Main theorem

Theorem

There is an explicitly computable function B of the complexity of finite sets of difference equations (e.g. number of variables, orders, total degrees, number of equations) so that for any difference field K and set $S \subseteq K\{\mathbf{x}, \mathbf{y}\}_\sigma$ of difference equations, so that if the difference elimination ideal of S is nontrivial, then so is the elimination ideal of $[S]_B$.

- When $m = 0$ (*i.e.*, when there are no $\mathbf{y}$ variables), by the Nullstellensatz, this gives a first-order condition for the existence of solutions to S in some sequence ring $L^{\mathbb{N}}$ with $L = L^{\mathrm{alg}}$ extending K and uncountable.
- The function B grows very quickly for underdetermined systems, but for practical elimination problems it tends to produce very small numbers.
- To ease notation, I will focus on the case where $m = 0$, but we should remember that for the applied parameter identification problems, the main point is to allow m to be large but the equations in $\mathbf{x}$ should be

Geometrizing the problem

- Let us focus on the consistency problem. It turns out that a solution to the elimination problem may be derived from this. For the sake of exposition, we work with difference equations with constant coefficients.
- As in the case of difference equations over fields, at the cost of adding more variables, we may reduce to the problem of dealing with order one equations. So we have polynomials $f_1(\mathsf{x}, \mathsf{x}'), \ldots, f_\ell(\mathsf{x}, \mathsf{x}')$ in $2N$ variables and wish to know whether we can find sequences so that $f_j(\mathbf{b}_n, \mathbf{b}_{n+1}) = 0$ for $1 \leq j \leq \ell$ and $n \in \mathbb{N}$.
- Let X be the algberaic variety defined by $f_1, \ldots, f_\ell$, and π_1 and π_2 be the projections to the first N (respectively, last N) coordinated restricted to X. We are looking for sequences (a_n) with $\mathsf{a}_n \in X$ and $\pi_2(\mathsf{a}_n) = \pi_1(\mathsf{a}_{n+1})$.
- In the case of fields, the geometric axioms say that such a solution exists just in case we eventually reduce to the situation that π_1 and π_2 are dominant to the same variety; for sequences it is much more complicated.

Geometrizing the problem

- Let us focus on the consistency problem. It turns out that a solution to the elimination problem may be derived from this. For the sake of exposition, we work with difference equations with constant coefficients.
- As in the case of difference equations over fields, at the cost of adding more variables, we may reduce to the problem of dealing with order one equations. So we have polynomials $f_1(\mathbf{x}, \mathbf{x}'), \ldots, f_\ell(\mathbf{x}, \mathbf{x}')$ in $2N$ variables and wish to know whether we can find sequences so that $f_j(\mathbf{b}_n, \mathbf{b}_{n+1}) = 0$ for $1 \leq j \leq \ell$ and $n \in \mathbb{N}$.
- Let X be the algberaic variety defined by $f_1, \ldots, f_\ell$, and π_1 and π_2 be the projections to the first N (respectively, last N) coordinated restricted to X. We are looking for sequences $(\mathbf{a}_n)$ with $\mathbf{a}_n \in X$ and $\pi_2(\mathbf{a}_n) = \pi_1(\mathbf{a}_{n+1})$.
- In the case of fields, the geometric axioms say that such a solution exists just in case we eventually reduce to the situation that π_1 and π_2 are dominant to the same variety; for sequences it is much more complicated.

Geometrizing the problem

- Let us focus on the consistency problem. It turns out that a solution to the elimination problem may be derived from this. For the sake of exposition, we work with difference equations with constant coefficients.
- As in the case of difference equations over fields, at the cost of adding more variables, we may reduce to the problem of dealing with order one equations. So we have polynomials $f_1(\mathbf{x}, \mathbf{x}'), \ldots, f_\ell(\mathbf{x}, \mathbf{x}')$ in $2N$ variables and wish to know whether we can find sequences so that $f_j(\mathbf{b}_n, \mathbf{b}_{n+1}) = 0$ for $1 \leq j \leq \ell$ and $n \in \mathbb{N}$.
- Let X be the algberaic variety defined by $f_1, \ldots, f_\ell$, and π_1 and π_2 be the projections to the first N (respectively, last N) coordinated restricted to X. We are looking for sequences $(\mathbf{a}_n)$ with $\mathbf{a}_n \in X$ and $\pi_2(\mathbf{a}_n) = \pi_1(\mathbf{a}_{n+1})$.
- In the case of fields, the geometric axioms say that such a solution exists just in case we eventually reduce to the situation that π_1 and π_2 are dominant to the same variety; for sequences it is much more complicated.

Geometrizing the problem

- Let us focus on the consistency problem. It turns out that a solution to the elimination problem may be derived from this. For the sake of exposition, we work with difference equations with constant coefficients.
- As in the case of difference equations over fields, at the cost of adding more variables, we may reduce to the problem of dealing with order one equations. So we have polynomials $f_1(\mathbf{x}, \mathbf{x}'), \ldots, f_\ell(\mathbf{x}, \mathbf{x}')$ in $2N$ variables and wish to know whether we can find sequences so that $f_j(\mathbf{b}_n, \mathbf{b}_{n+1}) = 0$ for $1 \leq j \leq \ell$ and $n \in \mathbb{N}$.
- Let X be the algberaic variety defined by $f_1, \ldots, f_\ell$, and π_1 and π_2 be the projections to the first N (respectively, last N) coordinated restricted to X. We are looking for sequences $(\mathbf{a}_n)$ with $\mathbf{a}_n \in X$ and $\pi_2(\mathbf{a}_n) = \pi_1(\mathbf{a}_{n+1})$.
- In the case of fields, the geometric axioms say that such a solution exists just in case we eventually reduce to the situation that π_1 and π_2 are dominant to the same variety; for sequences it is much more complicated.

Trains

Given our difference equation (X, π_1, π_2) a train of length $\ell \leq \infty$ is a sequence $(Y_j)_{j=1}^{\ell}$ of irreducible subvarieties of X such that $\overline{\pi_2 Y_j} = \overline{\pi_1 Y_{j+1}}$ for all j.

The information of a solution is equivalent to that of an infinite train of zero-dimensional varieites.

Our main technical result is to compute bounds so that if there is no infinite train, then there is no train longer than our bound. Indeed, we can arrange that if an infinite train exists, then it can be taken to be periodic of bounded period.

Trains

Given our difference equation (X, π_1, π_2) a train of length $\ell \leq \infty$ is a sequence $(Y_j)_{j=1}^{\ell}$ of irreducible subvarieties of X such that $\overline{\pi_2 Y_j} = \overline{\pi_1 Y_{j+1}}$ for all j.

The information of a solution is equivalent to that of an infinite train of zero-dimensional varieites.

Our main technical result is to compute bounds so that if there is no infinite train, then there is no train longer than our bound. Indeed, we can arrange that if an infinite train exists, then it can be taken to be periodic of bounded period.

Trains

Given our difference equation (X, π_1, π_2) a train of length $\ell \leq \infty$ is a sequence $(Y_j)_{j=1}^{\ell}$ of irreducible subvarieties of X such that $\overline{\pi_2 Y_j} = \overline{\pi_1 Y_{j+1}}$ for all j.

The information of a solution is equivalent to that of an infinite train of zero-dimensional varieites.

Our main technical result is to compute bounds so that if there is no infinite train, then there is no train longer than our bound. Indeed, we can arrange that if an infinite train exists, then it can be taken to be periodic of bounded period.

Axiomatizing solvability in $K^{\mathbb{Z}}$ with K an arbitrary algebraically closed field?

From the main technical result, we have another equivalent condition to the solvability of a system of difference equations in some difference ring extension: the associated geometric problem (X, π_1, π_2) admits an explicitly computable (skew-)periodic train $(Y_n)_{n=0}^{\infty}$ of explicitly bounded (skew-)period k.

How hard can it be to produce a K-solution from this (skew-)periodic train?

To simplify the presentation, we take $k = 1$ and work with constant coefficients. That is, $Y_n = Y_1$ for all n.

We start with $a_0 \in Y_0(K)$. To continue, we need to find $a_1 \in Y_1(K)$ with $\pi_1(a_1) = \pi_2(a_0)$. We know that $\overline{\pi_2(Y_0)} = \overline{\pi_1(Y_1)}$. So, for almost any choice of a_0, we can find the a_1. Adjust the first choice accordingly. Continuing, we find that almost any finite sequence may be extended, but the possible exceptional set is not under control.

Axiomatizing solvability in $K^{\mathbb{Z}}$ with K an arbitrary algebraically closed field?

From the main technical result, we have another equivalent condition to the solvability of a system of difference equations in some difference ring extension: the associated geometric problem (X, π_1, π_2) admits an explicitly computable (skew-)periodic train $(Y_n)_{n=0}^{\infty}$ of explicitly bounded (skew-)period k.

How hard can it be to produce a K-solution from this (skew-)periodic train?

To simplify the presentation, we take $k = 1$ and work with constant coefficients. That is, $Y_n = Y_1$ for all n.

We start with $a_0 \in Y_0(K)$. To continue, we need to find $a_1 \in Y_1(K)$ with $\pi_1(a_1) = \pi_2(a_0)$. We know that $\overline{\pi_2(Y_0)} = \overline{\pi_1(Y_1)}$. So, for almost any choice of a_0, we can find the a_1. Adjust the first choice accordingly. Continuing, we find that almost any finite sequence may be extended, but the possible exceptional set is not under control.

Axiomatizing solvability in $K^{\mathbb{Z}}$ with K an arbitrary algebraically closed field?

From the main technical result, we have another equivalent condition to the solvability of a system of difference equations in some difference ring extension: the associated geometric problem (X, π_1, π_2) admits an explicitly computable (skew-)periodic train $(Y_n)_{n=0}^{\infty}$ of explicitly bounded (skew-)period k.

How hard can it be to produce a K-solution from this (skew-)periodic train?

To simplify the presentation, we take $k = 1$ and work with constant coefficients. That is, $Y_n = Y_1$ for all n.

We start with $a_0 \in Y_0(K)$. To continue, we need to find $a_1 \in Y_1(K)$ with $\pi_1(a_1) = \pi_2(a_0)$. We know that $\overline{\pi_2(Y_0)} = \overline{\pi_1(Y_1)}$. So, for almost any choice of a_0, we can find the a_1. Adjust the first choice accordingly. Continuing, we find that almost any finite sequence may be extended, but the possible exceptional set is not under control.

Axiomatizing solvability in $K^{\mathbb{Z}}$ with K an arbitrary algebraically closed field?

From the main technical result, we have another equivalent condition to the solvability of a system of difference equations in some difference ring extension: the associated geometric problem (X, π_1, π_2) admits an explicitly computable (skew-)periodic train $(Y_n)_{n=0}^{\infty}$ of explicitly bounded (skew-)period k.

How hard can it be to produce a K-solution from this (skew-)periodic train?

To simplify the presentation, we take $k = 1$ and work with constant coefficients. That is, $Y_n = Y_1$ for all n.

We start with $a_0 \in Y_0(K)$. To continue, we need to find $a_1 \in Y_1(K)$ with $\pi_1(a_1) = \pi_2(a_0)$. We know that $\overline{\pi_2(Y_0)} = \overline{\pi_1(Y_1)}$. So, for almost any choice of a_0, we can find the a_1. Adjust the first choice accordingly. Continuing, we find that almost any finite sequence may be extended, but the possible exceptional set is not under control.

(Skew-)periodic points

Continuing with the same notation, if we could find a point a_0 so that $\sigma(a_0) \in Y_1(K)$ and $\pi_1(\sigma(a_0)) = \pi_2(a_0)$, then we could produce a sequence solution.

This might be impossible for our given (K, σ). It may happen that σ acts trivially on K, for instance, and that the equations $x \in Y_0$ and $\pi_1(x) = \pi_2(x)$ are inconsistent.

However, in an existentially closed difference field, these solutions do exist. Thus, from the limit theory of the Frobenius (that is, Hrushovski's theorem that if $\mathscr{U}$ is a nonprincipal ultrafilter on the set of prime powers, then the difference field $\prod_{\mathscr{U}} \mathbb{F}_q^{\mathrm{alg}}, x \mapsto x^q)$ is existentially closed), it follows that they may be found in a finite field with a power of the Frobenius, and a specialization argument permits us to lift them to K.

(Skew-)periodic points

Continuing with the same notation, if we could find a point a_0 so that $\sigma(a_0) \in Y_1(K)$ and $\pi_1(\sigma(a_0)) = \pi_2(a_0)$, then we could produce a sequence solution.

This might be impossible for our given (K, σ). It may happen that σ acts trivially on K, for instance, and that the equations $x \in Y_0$ and $\pi_1(x) = \pi_2(x)$ are inconsistent.

However, in an existentially closed difference field, these solutions do exist. Thus, from the limit theory of the Frobenius (that is, Hrushovski's theorem that if $\mathscr{U}$ is a nonprincipal ultrafilter on the set of prime powers, then the difference field $\prod_{\mathscr{U}} \mathbb{F}_q^{\mathrm{alg}}, x \mapsto x^q)$ is existentially closed), it follows that they may be found in a finite field with a power of the Frobenius, and a specialization argument permits us to lift them to K.

(Skew-)periodic points

Continuing with the same notation, if we could find a point a_0 so that $\sigma(a_0) \in Y_1(K)$ and $\pi_1(\sigma(a_0)) = \pi_2(a_0)$, then we could produce a sequence solution.

This might be impossible for our given (K, σ). It may happen that σ acts trivially on K, for instance, and that the equations $x \in Y_0$ and $\pi_1(x) = \pi_2(x)$ are inconsistent.

However, in an existentially closed difference field, these solutions do exist. Thus, from the limit theory of the Frobenius (that is, Hrushovski's theorem that if $\mathscr{U}$ is a nonprincipal ultrafilter on the set of prime powers, then the difference field $\prod_{\mathscr{U}} \mathbb{F}_q^{\mathrm{alg}}, x \mapsto x^q)$ is existentially closed), it follows that they may be found in a finite field with a power of the Frobenius, and a specialization argument permits us to lift them to K.

(Skew-)periodic points

Continuing with the same notation, if we could find a point a_0 so that $\sigma(a_0) \in Y_1(K)$ and $\pi_1(\sigma(a_0)) = \pi_2(a_0)$, then we could produce a sequence solution.

This might be impossible for our given (K, σ). It may happen that σ acts trivially on K, for instance, and that the equations $x \in Y_0$ and $\pi_1(x) = \pi_2(x)$ are inconsistent.

However, in an existentially closed difference field, these solutions do exist. Thus, from the limit theory of the Frobenius (that is, Hrushovski's theorem that if $\mathscr{U}$ is a nonprincipal ultrafilter on the set of prime powers, then the difference field $\prod_{\mathscr{U}} \mathbb{F}_q^{\mathrm{alg}}, x \mapsto x^q)$ is existentially closed), it follows that they may be found in a finite field with a power of the Frobenius, and a specialization argument permits us to lift them to K.

Concluding remarks and questions

- In our application of Hrushovski's theorem on the limit theory of the Frobenius we make use of a weaker published theorem of [Varshavsky, *J. Alg. Geom.*, 2018] where all the data are defined over a finite field. Is this weaker theorem enough to recover the result that ACFA is the limit theory of the Frobenius?
- There is still a gap between our positive result on the decidability of consistency of difference equations with coefficients from a difference field and the undecidability of the theory of sequence rings. Where is the border between the class of coefficient rings for which the solution to this problem may be axiomatized and those where it cannot? Here we are deciding positive existential formulae. Is the full existential theory decidable?
- In the follow up work with Wei Li, we extend these methods to difference-differential equations. The theoretical results are similar, but the bounds we compute are much worse.

Concluding remarks and questions

- In our application of Hrushovski's theorem on the limit theory of the Frobenius we make use of a weaker published theorem of [Varshavsky, *J. Alg. Geom.*, 2018] where all the data are defined over a finite field. Is this weaker theorem enough to recover the result that ACFA is the limit theory of the Frobenius?
- There is still a gap between our positive result on the decidability of consistency of difference equations with coefficients from a difference field and the undecidability of the theory of sequence rings. Where is the border between the class of coefficient rings for which the solution to this problem may be axiomatized and those where it cannot? Here we are deciding positive existential formulae. Is the full existential theory decidable?
- In the follow up work with Wei Li, we extend these methods to difference-differential equations. The theoretical results are similar, but the bounds we compute are much worse.

Concluding remarks and questions

- In our application of Hrushovski's theorem on the limit theory of the Frobenius we make use of a weaker published theorem of [Varshavsky, *J. Alg. Geom.*, 2018] where all the data are defined over a finite field. Is this weaker theorem enough to recover the result that ACFA is the limit theory of the Frobenius?
- There is still a gap between our positive result on the decidability of consistency of difference equations with coefficients from a difference field and the undecidability of the theory of sequence rings. Where is the border between the class of coefficient rings for which the solution to this problem may be axiomatized and those where it cannot? Here we are deciding positive existential formulae. Is the full existential theory decidable?
- In the follow up work with Wei Li, we extend these methods to difference-differential equations. The theoretical results are similar, but the bounds we compute are much worse.

Concluding remarks and questions

- In our application of Hrushovski's theorem on the limit theory of the Frobenius we make use of a weaker published theorem of [Varshavsky, *J. Alg. Geom.*, 2018] where all the data are defined over a finite field. Is this weaker theorem enough to recover the result that ACFA is the limit theory of the Frobenius?
- There is still a gap between our positive result on the decidability of consistency of difference equations with coefficients from a difference field and the undecidability of the theory of sequence rings. Where is the border between the class of coefficient rings for which the solution to this problem may be axiomatized and those where it cannot? Here we are deciding positive existential formulae. Is the full existential theory decidable?
- In the follow up work with Wei Li, we extend these methods to difference-differential equations. The theoretical results are similar, but the bounds we compute are much worse.