Solving equations in sequences: cans and cannots

Gleb Pogudin (LIX, CNRS, École Polytechnique, IPP)
joint with A. Ovchinnikov, T. Scanlon, and M. Wibmer

INSTITUT POLYTECHNIQUE DE PARIS

Big picture

Difference equations are used in combinatorics, number theory, and to model discrete-time processes, etc.

Big picture

Difference equations are used in combinatorics, number theory, and to model discrete-time processes, etc.

Often, solutions in sequences are of interest.

Big picture

Difference equations are used in combinatorics, number theory, and to model discrete-time processes, etc.

Often, solutions in sequences are of interest.

In this talk:

- algorithm for checking consistency of a system of equations (and elimination),
- undecidability results for almost anything beyond,
- and speculation.

Part 1: Prologue

Main characters and first obstacles

Difference equations and their solutions

- $F_{n+2} = F_{n+1} + F_n$
  Solution: $\{\dots, 1, 0, 1, 1, 2, 3, 5, 8, 13, \dots\}$ in the ring $\mathbb{C}^{\mathbb{Z}}$ of sequences

Difference equations and their solutions

- $F_{n+2} = F_{n+1} + F_n$
  Solution: $\{\ldots, 1, 0, 1, 1, 2, 3, 5, 8, 13, \ldots\}$ in the ring $\mathbb{C}^{\mathbb{Z}}$ of sequences
  More formally: $\sigma^2(F) = \sigma(F) + F$

Difference equations and their solutions

- $F_{n+2} = F_{n+1} + F_n$
  Solution: $\{\ldots, 1, 0, 1, 1, 2, 3, 5, 8, 13, \ldots\}$ in the ring $\mathbb{C}^{\mathbb{Z}}$ of sequences
  More formally: $\sigma^2(F) = \sigma(F) + F$

- $f(x+1) = xf(x)$
  Solution: $\Gamma(x)$ in the field of meromorphic functions on $\mathbb{C}$

Difference equations and their solutions

- $F_{n+2} = F_{n+1} + F_n$
  Solution: $\{\dots, 1, 0, 1, 1, 2, 3, 5, 8, 13, \dots\}$ in the ring $\mathbb{C}^{\mathbb{Z}}$ of sequences
  More formally: $\sigma^2(F) = \sigma(F) + F$

- $f(x+1) = xf(x)$
  Solution: $\Gamma(x)$ in the field of meromorphic functions on $\mathbb{C}$
  More formally: $\sigma(f) = xf$

Difference equations and their solutions

- $F_{n+2} = F_{n+1} + F_n$
  Solution: $\{\dots, 1, 0, 1, 1, 2, 3, 5, 8, 13, \dots\}$ in the ring $\mathbb{C}^{\mathbb{Z}}$ of sequences
  More formally: $\sigma^2(F) = \sigma(F) + F$

- $f(x+1) = xf(x)$
  Solution: $\Gamma(x)$ in the field of meromorphic functions on $\mathbb{C}$
  More formally: $\sigma(f) = xf$

- $\sigma(f) = 2f + 1$

Difference equations and their solutions

- $F_{n+2} = F_{n+1} + F_n$
  Solution: $\{\ldots, 1, 0, 1, 1, 2, 3, 5, 8, 13, \ldots\}$ in the ring $\mathbb{C}^{\mathbb{Z}}$ of sequences
  More formally: $\sigma^2(F) = \sigma(F) + F$

- $f(x+1) = xf(x)$
  Solution: $\Gamma(x)$ in the field of meromorphic functions on $\mathbb{C}$
  More formally: $\sigma(f) = xf$

- $\sigma(f) = 2f + 1$

$\boldsymbol{\sigma}$	**Equation**	**Solution**
shift on $\mathbb{C}^{\mathbb{Z}}$	$f_{n+1} = 2f_n + 1$	$\{\ldots, 0, 1, 3, 7, \ldots\}$

Difference equations and their solutions

- $F_{n+2} = F_{n+1} + F_n$
  Solution: $\{\dots, 1, 0, 1, 1, 2, 3, 5, 8, 13, \dots\}$ in the ring $\mathbb{C}^{\mathbb{Z}}$ of sequences
  More formally: $\sigma^2(F) = \sigma(F) + F$

- $f(x+1) = xf(x)$
  Solution: $\Gamma(x)$ in the field of meromorphic functions on $\mathbb{C}$
  More formally: $\sigma(f) = xf$

- $\sigma(f) = 2f + 1$

$\boldsymbol{\sigma}$	**Equation**	**Solution**
shift on $\mathbb{C}^{\mathbb{Z}}$	$f_{n+1} = 2f_n + 1$	$\{\dots, 0, 1, 3, 7, \dots\}$
shift on functions	$f(x+1) = 2f(x) + 1$	$2^x - 1$

Functions vs. sequences

Example

$$\begin{cases} f\sigma(f) = 0, \\ f + \sigma(f) = 1 \end{cases}$$

Functions vs. sequences

Example

$$\begin{cases} f\sigma(f) = 0, \\ f + \sigma(f) = 1 \end{cases}$$

- does not have a solution in meromorphic function in $\mathbb{C}$;

Functions vs. sequences

Example

$$\begin{cases} f\sigma(f) = 0, \\ f + \sigma(f) = 1 \end{cases}$$

- does not have a solution in meromorphic function in $\mathbb{C}$ (more generally, any difference field);

Functions vs. sequences

Example

$$\begin{cases} f\sigma(f) = 0, \\ f + \sigma(f) = 1 \end{cases}$$

- does not have a solution in meromorphic function in $\mathbb{C}$ (more generally, any difference field);
- has a solution $f = \{\ldots, 0, 1, 0, 1, \ldots\}$ is σ is a shift on $\mathbb{C}^{\mathbb{Z}}$.

Sequences vs. Germs

Germs

Let $\mathcal{I} := \{$sequences in $\mathbb{C}^{\mathbb{Z}}$ with finite support$\}$, this is an ideal.

Sequences vs. Germs

Germs
Let $\mathcal{I} := \{\text{sequences in } \mathbb{C}^{\mathbb{Z}} \text{ with finite support}\}$, this is an ideal.

Ring of germs: $\mathcal{G} := \mathbb{C}^{\mathbb{Z}}/\mathcal{I}$.

Sequences vs. Germs

Germs

Let $\mathcal{I} := \{\text{sequences in } \mathbb{C}^{\mathbb{Z}} \text{ with finite support}\}$, this is an ideal.

Ring of germs: $\mathcal{G} := \mathbb{C}^{\mathbb{Z}}/\mathcal{I}$.

Example

Consider $f \cdot g = 0$ & $f \neq 0$.

Sequences vs. Germs

Germs
Let $\mathcal{I} := \{\text{sequences in } \mathbb{C}^{\mathbb{Z}} \text{ with finite support}\}$, this is an ideal.

Ring of germs: $\mathcal{G} := \mathbb{C}^{\mathbb{Z}}/\mathcal{I}$.

Example

Consider $f \cdot g = 0$ & $f \neq 0$.

- in sequences: g contains at least one zero;

Sequences vs. Germs

Germs
Let $\mathcal{I} := \{\text{sequences in } \mathbb{C}^{\mathbb{Z}} \text{ with finite support}\}$, this is an ideal.

Ring of germs: $\mathcal{G} := \mathbb{C}^{\mathbb{Z}}/\mathcal{I}$.

Example

Consider $f \cdot g = 0$ & $f \neq 0$.

- in sequences: g contains at least one zero;
- in germs: g contains infinitely many zeros.

Not an easy solution space!

Theorem (Hrushovski, Point, 2007)

Problem:

- given a system of difference equations and inequations
- check if it has a solution.

Is undecidable both in $\mathbb{C}^{\mathbb{Z}}$ and $\mathcal{G}$.

Not an easy solution space!

Theorem (Hrushovski, Point, 2007)

Problem:

- given a system of difference equations and inequations
- check if it has a solution.

Is undecidable both in $\mathbb{C}^{\mathbb{Z}}$ and $\mathcal{G}$.

Glimpse under the hood

Encoding diophantine equations:

$$f \cdot g = 0 \;\&\; g \neq 0 \;\&\; (f - \sigma(f))^2 = 1$$

implies that f consists of integers.

Not an easy solution space!

Theorem (Hrushovski, Point, 2007)

Problem:

- given a system of difference equations and inequations
- check if it has a solution.

Is undecidable both in $\mathbb{C}^{\mathbb{Z}}$ and $\mathcal{G}$.

Glimpse under the hood

Encoding diophantine equations:

$$f \cdot g = 0 \,\&\, g \neq 0 \,\&\, (f - \sigma(f))^2 = 1$$

implies that f consists of integers. Then

$$h = \sigma(h) \,\&\, (h - f) \cdot e = 0 \,\&\, e \neq 0$$

implies that h is a constant integer sequence.

Part 2: Cans

Consistency and elimination

joint with A. Ovchinnikov and T. Scanlon

`https://arxiv.org/abs/1712.01412`

Consistency problem

- Given a system of difference equations over $\mathbb{C}$
- Check if it has a solution.

Consistency problem

- Given a system of difference equations over $\mathbb{C}$
- Check if it has a solution.

Question: solution where?

$\mathbb{C}^{\mathbb{Z}}$ or nothing

$\mathbb{C}^{\mathbb{Z}}$ or nothing

Theorem (Ovchinnikov, Pogudin, Scanlon, 2020)

System of difference equations over a constant field k has a solution in some difference ring	$\Longrightarrow$	It has a solution in $\bar{k}^{\mathbb{Z}}$

How to detect inconsistency?

Example

Does there exist a sequence $\{a_n\}_{n\in\mathbb{Z}}$ such that:

$$\begin{cases} a_{n+4} = a_n, \\ a_{n+5} = a_n + 1 \end{cases} \quad ?$$

How to detect inconsistency?

Example

Does there exist a sequence $\{a_n\}_{n\in\mathbb{Z}}$ such that:

$$\begin{cases} a_{n+4} = a_n, \\ a_{n+5} = a_n + 1 \end{cases} ?$$

NO because

$$a_{20} = a_0 \quad \text{and} \quad a_{20} = a_0 + 4.$$

How to detect inconsistency?

Example

Does there exist a sequence $\{a_n\}_{n\in\mathbb{Z}}$ such that:

$$\begin{cases} a_{n+4} = a_n, \\ a_{n+5} = a_n + 1 \end{cases} ?$$

NO because

$$a_{20} = a_0 \quad \text{and} \quad a_{20} = a_0 + 4.$$

Idea: no "finite" solution $\implies$ no solution.

How to detect inconsistency?

Example

Does there exist a sequence $\{a_n\}_{n\in\mathbb{Z}}$ such that:

$$\begin{cases} a_{n+4} = a_n, \\ a_{n+5} = a_n + 1 \end{cases} \quad ?$$

NO because

$$a_{20} = a_0 \quad \text{and} \quad a_{20} = a_0 + 4.$$

Idea: no "finite" solution $\implies$ no solution. Converse? Bound?

Converse — yes

Theorem (OPS, 2020)

Finite solution of any length $\implies$ infinite solution.

Converse — yes

Theorem (OPS, 2020)

Finite solution of any length $\implies$ infinite solution.

Small $\neq$ easy

Surprisingly hard over "small" fields (e.g., $\mathbb{Q}$ or $\mathbb{F}_p$, not $\mathbb{C}$).

Converse — yes

Theorem (OPS, 2020)

Finite solution of any length $\implies$ infinite solution.

Small $\neq$ easy

Surprisingly hard over "small" fields (e.g., $\mathbb{Q}$ or $\mathbb{F}_p$, not $\mathbb{C}$).

Involves

- parts of the proof of bound (coming soon);
- nonstandard Frobenius as a model of ACFA.

Algorithm: first try

Idea: difference equations $\implies$ polynomial equations
via prolongation

Algorithm: first try

Idea: difference equations $\implies$ polynomial equations
via prolongation

Possible approach

1. Apply shift $n \mapsto n+1$ (a prolongation) to the system
2. Check consistency of the polynomial system
3. If not succeed, go to Step 1.

Algorithm: first try

Idea: difference equations $\Longrightarrow$ polynomial equations
via prolongation

Possible approach

1. Apply shift $n \mapsto n+1$ (a prolongation) to the system
2. Check consistency of the polynomial system
3. If not succeed, go to Step 1.

Half-solution: can detect inconsistency but not consistency.

Bound for the number of prolongations

Theorem (OPS, 2020)

If the system is inconsistent, this will be detected after at most

$$\mathbf{N} = B(d, D)$$

prolongations, where

D the degree of the system,

d the dimension of the system.

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

Example (sharpness for $d = 0$)

Theorem implies that $B(0, D) = D + 1$.

Example (sharpness for $d = 0$)

Theorem implies that $B(0, D) = D + 1$.

This value is achieved on the elimination problem of x_i in

$$\begin{cases} x_{i+1} = x_i + 1, \\ x_i \cdot (x_i - 1) \ldots \cdot (x_i - D + 1) = 0. \end{cases}$$

How to detect consistency?

Example (periodicity)

$$a_n(a_n - 1)(a_n - 2) = 0 \quad \text{and} \quad (a_{n+1} - a_n)^2 = 1.$$

There is a periodic solution

How to detect consistency?

Example (periodicity)

$$a_n(a_n - 1)(a_n - 2) = 0 \quad \text{and} \quad (a_{n+1} - a_n)^2 = 1.$$

There is a periodic solution $0, 1, 0, 1, 0, 1, \ldots$

How to detect consistency?

Example (periodicity)

$$a_n(a_n - 1)(a_n - 2) = 0 \quad \text{and} \quad (a_{n+1} - a_n)^2 = 1.$$

There is a periodic solution $0, 1, 0, 1, 0, 1, \ldots$

Idea: prove there is always a periodic solution + bound the period

How to detect consistency?

Example (periodicity)

$$a_n(a_n-1)(a_n-2)=0 \quad \text{and} \quad (a_{n+1}-a_n)^2=1.$$

There is a periodic solution $0,1,0,1,0,1,\ldots$

Idea: prove there is always a periodic solution + bound the period

BUT $a_{n+1}=a_n+1$ does not have periodic solutions

How to detect consistency?

Example (periodicity)

$$a_n(a_n - 1)(a_n - 2) = 0 \quad \text{and} \quad (a_{n+1} - a_n)^2 = 1.$$

There is a periodic solution $0, 1, 0, 1, 0, 1, \ldots$

Idea: prove there is always a periodic solution + bound the period

BUT $a_{n+1} = a_n + 1$ does not have periodic solutions

Next idea: allow solutions to contain "high-dimensional points"
For example: $\mathbb{A} = \mathbb{A} + 1$, so $\{a_n\} = \{\mathbb{A}, \mathbb{A}, \ldots\}$ is a periodic solution

Picture

We can bring every system to a form

$(a_n + b_n)(a_n - b_n) = 0$	–	nonlinear but no shifts
$b_{n+1} = a_n$	–	with a shift but linear

Conjectures/expectations

- Seems that the main issue — combinatorics;

Conjectures/expectations

- Seems that the main issue — combinatorics;
- Sharpness in $d = 0$ and bound for $d = 1$ indicate that the worst case is a union of hyperplanes;

Conjectures/expectations

- Seems that the main issue — combinatorics;
- Sharpness in $d = 0$ and bound for $d = 1$ indicate that the worst case is a union of hyperplanes;
- Possible approach
  - consider the "worst" case, union of hypersurfaces, get lower bounds;
  - employ deformation argument to reduce general case to unions of hyperplanes.

Part 3: Cannots

Implications, grids, $\mathbb{R}$

joint with T. Scanlon and M. Wibmer

https://arxiv.org/abs/1909.03239

Checking implication

Problem

- Given a system of difference equations $f_1 = \ldots = f_\ell = 0$ and one more equation $g = 0$
- Check if $g = 0$ holds for any solution of $f_1 = \ldots = f_\ell = 0$.

Checking implication

Problem

- Given a system of difference equations $f_1 = \ldots = f_\ell = 0$ and one more equation $g = 0$
- Check if $g = 0$ holds for any solution of $f_1 = \ldots = f_\ell = 0$.

Connection to Hrushovski-Point

Problem above $\iff$ consistency of $f_1 = \ldots = f_\ell = 0$ & $g \neq 0$

Checking implication

Problem

- Given a system of difference equations $f_1 = \ldots = f_\ell = 0$ and one more equation $g = 0$
- Check if $g = 0$ holds for any solution of $f_1 = \ldots = f_\ell = 0$.

Connection to Hrushovski-Point

Problem above $\iff$ consistency of $f_1 = \ldots = f_\ell = 0$ & $g \neq 0$

In Hrushovski-Point case many inequations, here just one.

Checking implication

Problem

- Given a system of difference equations $f_1 = \ldots = f_\ell = 0$ and one more equation $g = 0$
- Check if $g = 0$ holds for any solution of $f_1 = \ldots = f_\ell = 0$.

Connection to Hrushovski-Point

Problem above $\iff$ consistency of $f_1 = \ldots = f_\ell = 0$ & $g \neq 0$

In Hrushovski-Point case many inequations, here just one.

Theorem (PSW, 2020)

If solutions are sought in sequences, the problem is undecidable.

Checking implication

Problem

- Given a system of difference equations $f_1 = \ldots = f_\ell = 0$ and one more equation $g = 0$
- Check if $g = 0$ holds for any solution of $f_1 = \ldots = f_\ell = 0$.

Connection to Hrushovski-Point

Problem above $\iff$ consistency of $f_1 = \ldots = f_\ell = 0$ & $g \neq 0$

In Hrushovski-Point case many inequations, here just one.

Theorem (PSW, 2020)

If solutions are sought in sequences, the problem is undecidable.

Idea: system $\implies$ piecie-wise polynomial map $\implies$ enumerating tuples of integers $\implies$ diophantine equations

Consistency over reals

Problem

- Given a system of difference equations over $\mathbb{R}$
- Check if it has a solution in $\mathbb{R}^{\mathbb{Z}}$.

Consistency over reals

Problem

- Given a system of difference equations over $\mathbb{R}$
- Check if it has a solution in $\mathbb{R}^{\mathbb{Z}}$.

Theorem (PSW, 2020)

The problem is undecidable.

Consistency over reals

Problem

- Given a system of difference equations over $\mathbb{R}$
- Check if it has a solution in $\mathbb{R}^{\mathbb{Z}}$.

Theorem (PSW, 2020)

The problem is undecidable.

About the proof

In Hrushovski-Point: inequations used for "$\{a_n\}$ contains infinitely many zeroes". We do this in $\mathbb{R}$ (with Lagrange four-square theorem!).

Equations on grids

Consider equations with two shifts like
$a_{m,n} = \frac{1}{4}(a_{m-1,n} + a_{m,n-1} + a_{m+1,n} + a_{m,n+1})$.

Equations on grids

Consider equations with two shifts like
$a_{m,n} = \frac{1}{4}(a_{m-1,n} + a_{m,n-1} + a_{m+1,n} + a_{m,n+1})$.

Problem

- Given a system of difference equations over $\mathbb{C}$ with two shifts
- Check if it has a solution in $\mathbb{C}^{\mathbb{Z}^2}$.

Equations on grids

Consider equations with two shifts like
$a_{m,n} = \frac{1}{4}(a_{m-1,n} + a_{m,n-1} + a_{m+1,n} + a_{m,n+1})$.

Problem

- Given a system of difference equations over $\mathbb{C}$ with two shifts
- Check if it has a solution in $\mathbb{C}^{\mathbb{Z}^2}$.

Theorem (PSW, 2020)

The problem is undecidable.

Equations on grids

Consider equations with two shifts like
$a_{m,n} = \frac{1}{4}(a_{m-1,n} + a_{m,n-1} + a_{m+1,n} + a_{m,n+1})$.

Problem

- Given a system of difference equations over $\mathbb{C}$ with two shifts
- Check if it has a solution in $\mathbb{C}^{\mathbb{Z}^2}$.

Theorem (PSW, 2020)

The problem is undecidable.

About the proof

Reduction to the domino tiling problem.

Equations on grids

Consider equations with two shifts like
$a_{m,n} = \frac{1}{4}(a_{m-1,n} + a_{m,n-1} + a_{m+1,n} + a_{m,n+1})$.

Problem

- Given a system of difference equations over $\mathbb{C}$ with two shifts
- Check if it has a solution in $\mathbb{C}^{\mathbb{Z}^2}$.

Theorem (PSW, 2020)

The problem is undecidable.

About the proof

Reduction to the domino tiling problem.

Remark: similar result if the sequences are indexed by a free monoid.

End of the story? Of course, no

- The undecidability-of-implication proof does not work for germs. Still decidable?

End of the story? Of course, no

- The undecidability-of-implication proof does not work for germs. Still decidable?
- Many interesting algebraically closed field: p-adics, $\mathbb{F}_p(t)$, etc

End of the story? Of course, no

- The undecidability-of-implication proof does not work for germs. Still decidable?
- Many interesting algebraically closed field: p-adics, $\mathbb{F}_p(t)$, etc
- Shink the class of sequences: the ones that may "come from discretization"?

Summary

- Cold start: known undecidability of equations + inequations

Summary

- Cold start: known undecidability of equations + inequations
- New hope: algorithm for equations
  (+ bound, + universality, + elimination)

Summary

- Cold start: known undecidability of equations + inequations
- New hope: algorithm for equations
  (+ bound, + universality, + elimination)
- Understanding the limits: undecidability for implications, reals, equations on grids

Summary

- Cold start: known undecidability of equations + inequations
- New hope: algorithm for equations
  (+ bound, + universality, + elimination)
- Understanding the limits: undecidability for implications, reals, equations on grids
- Still many promising directions!

Thank you!

Looking for a PhD student: http://www.lix.polytechnique.fr/Labo/Gleb.POGUDIN/phd-occam/