Solving equation systems in ω-categorical algebras

Thomas Quinn-Gregson
TU Dresden
Joint work with Manuel Bodirsky

European Research Council
Established by the European Commission

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No.681988)

Our problem

Given an algebra A, we are interested in the problem of deciding whether a given system of term equalities and inequalities has a solution in A.

Example

Let L be a left zero semigroup. Does the following system have a solution over $(L; \cdot)$?

$$
\begin{aligned}
x_1 \cdot x_2 &= x_3 \cdot x_4, \\
x_3 \cdot x_4 \cdot x_5 &= x_2, \\
x_2 \cdot x_5 &\neq x_1 \cdot x_3.
\end{aligned}
$$

Equivalent: does $x_1 = x_3, x_3 = x_2, x_2 \neq x_1$ have a solution in $(|L|; \neq)$?

- Given an algebra A, can we create a "fast" algorithm which solves any given system over A?
- **Spoilers:** The problem for a left zero semigroup is solvable in polynomial time when $|L| = 1, 2$ or infinite.

Part 1: CSPs

A rough definition

A **constraint satisfaction problem** consists of:

1. a finite list of variables V,
2. a domain of possible values A,
3. a set of constraints on those variables $\mathcal{C}$.

Problem: Can we assign values to all the variables so that all the constraints are satisfied?

Example (Graph 3-colouring)

Let G be a finite graph. Each vertex can be coloured either red, green or blue. Problem: can we colour G such that no two adjacent variables have the same colour?
$V =$ vertices of G.
$A = \{\text{Red, Green, Blue}\}$.
$\mathcal{C} =$ "no two adjacent vertices have the same colour".

Constraint language

Much attention has been paid to the case where the constraints arise from finitely many relations and functions on a fixed domain.

Definition

Given a (first-order) structure $(A; \Gamma)$ where Γ is finite, we define $\mathrm{CSP}(A; \Gamma)$, or simply $\mathrm{CSP}(\Gamma)$, to be the CSP with:

- **Instance:** $I = (V, A, \mathcal{C})$ in which each constraint is simply a relation from Γ.
- **Question:** Does I have a solution?

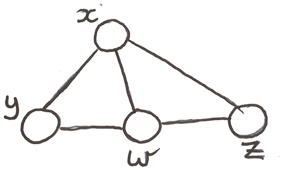
Example

Graph 3-colouring can be considered as $\mathrm{CSP}(A; \neq)$ where $A = \{R, B, G\}$ i.e. $\mathrm{CSP}(K_3)$, where K_3 is the complete graph on 3 vertices.

Graph 3-colouring

Instance: $x \neq y$, $x \neq z$, $x \neq w$,
$y \neq w$, $z \neq w$.

Graph:

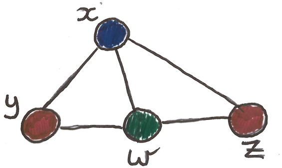


Q: Can we colour the vertices Red, Blue or Green such that no adjacent vertices are the same colour?

3-Graph colouring

Instance: $x \neq y$, $x \neq z$, $x \neq w$, $y \neq w$, $z \neq w$.

Graph:



Q^{n}: Can we colour the vertices Red, Blue or Green such that no adjacent vertices are the same colour?

Computational Complexity

Key question: How does the structure $\mathcal{A}$ affect the computational complexity of CSP($\mathcal{A}$)?

Definition

1. *P*: the class of all problems solved in polynomial time. Its members are called **tractable**.
2. *NP*: the class of problems solvable in nondeterministic polynomial time.
3. *NP*-hard: the class of problems which at least as hard as the hardest problems in *NP*.
4. *NP*-complete: the class of problems which are *NP* and *NP*-hard (the "hardest problems in *NP*").

Theorem (Ladner, 1975)

If $P \neq NP$ then there are problems in $NP \setminus P$ that are not NP-complete.

Dichotomy Theorem for finite structures

Example

Graph n-colouring is NP-complete if $n > 2$, and tractable otherwise. Equivalently, $\mathrm{CSP}(\mathbf{n};\neq) = \mathrm{CSP}(K_n)$ is NP-complete when $n > 2$, and tractable otherwise.

Example (Hell and Nešetři, 90')

Let G be a finite undirected graph. Then $\mathrm{CSP}(G)$ is either tractable (if bipartite) or NP-complete.

Theorem (Dichotomy Theorem (Bulatov, Zhuk 17'))

Let $\mathcal{A}$ be a finite structure. Then CSP($\mathcal{A}$) is either tractable or is NP-complete.

Part 2: CSPs arising from algebras

System of equations satisfactibility

Definition (The *system of equations satisfactibility* problem)

Given a finite algebra $\mathcal{A} = (A; F)$, the problem $\text{EQN}^*_{\mathcal{A}}$ is:
Instance: a system of equations $\mathcal{E}$ over $\mathcal{A}$ (constants and variables).
Question: does $\mathcal{E}$ have a solution?

Example

Consider the abelian group $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. An instance of $\text{EQN}^*_{\mathbb{Z}_5}$ could be

$$\begin{aligned} x + y &= 1, \\ z + u + 2 &= x + v, \\ u &= v + 1. \end{aligned}$$

Solve by Gaussian Elimination e.g. $x = v = 0, y = u = 1, z = 2$.

System of equations satisfactibility

The problem $\mathrm{EQN}^*_{\mathcal{A}}$ is equivalent to $\mathrm{CSP}(\mathcal{A}, c_1, \ldots, c_n)$ where $A = \{c_1, \ldots, c_n\}$.

Theorem (Goldmann, Russell 2002)

Let G be a finite group. If G is abelian then EQN^*_G is tractable, and is NP-complete otherwise.

Theorem (Klíma, Tesson, Thérien 2007)

Every CSP over a finite domain is polynomial-time equivalent to EQN^*_S for some finite semigroup S.

To infinity...

We are interested in building non-trivial CSPs from an infinite algebra $\mathcal{A} = (A; F)$. Possibilities include:

1. $\mathrm{EQN}^*_{\mathcal{A}}$

Pro: Natural problem.

Cons: $\mathrm{CSP}(\mathcal{A}, a : a \in A)$ has an infinite language.

2. Get rid of constants i.e. $\mathrm{CSP}(\mathcal{A})$.

Pros: Natural problem, finite language.

Con: Often a trivial problem e.g. if A is a group, then every equation can be solved by substituting in the identity element.

3. Replace constants by disequality i.e. $\mathrm{CSP}(\mathcal{A}, \neq)$

Pros: natural problem, finite language, non-trivial, core,...

Con: rather boring for finite algebras - NP-complete if $2 < |A| < \omega$.

Our problem

We study CSP$(A, \neq)$ for algebras A. Motivation include:

- **A natural problem:** CSP$(A, \neq)$ is polynomial time equivalent to the problem of deciding whether a given set of term equalities and inequalities has a solution in A.
- **A non-trivial problem:** As we will see, even in our very restrictive setting we obtain both tractability and hardness.
- **Constraint entailment:** Testing if a list of equations $\mathcal{E}$ implies an equation $u = v$ is equivalent of testing if $\mathcal{E} \cup \{u \neq v\}$ is satisfiable.
- **The Identity Checking Problem ICP(A)**: CSP$(A, \neq) \in P \Rightarrow$ ICP$(A) \in P$.
- **Sporadically studied problem:** CSP$(A, \neq)$ for a number of well-known algebras have served as key examples:
  - the lattice reduct of the atomless Boolean algebra $(\mathbb{A}; \cup, \cap)$ (NP-hard; Bodirsky, Hils, Krimkevitch, 2011)
  - the infinite-dimensional vector space over the finite field $\mathbb{F}_q$ (tractable; Bodirsky, Chen, Kára, von Oertzen, 2007).

ω-categoricity

Much progress has been made in understanding the CSPs of infinite structures: often in the (highly symmetric) ω-categorical setting.
e.g. If M and N are ω-categorical then CSP(M)=CSP(N) if and only if $M \to N$ and $N \to M$.

Definition

A structure M is ω-**categorical** if Th(M) has one countable model, up to isomorphism. Equivalently, if Aut(M) has only finitely many orbits on its action on M^n for each $n \geq 1$.

Example

A right zero semigroup S has $\text{Aut}(S) = \mathcal{S}_{|S|}$ and is ω-categorical:

- $\forall x, y, z \ [(xy)z = x(yz)]$
- $\forall x, y \ [xy = y]$
- 'correct cardinality'

ω-categoricity

Example

An abelian group is ω-categorical if and only if it has finite exponent i.e. $\exists n \in \mathbb{N}$ with $g^n = 1$ for all $g \in G$.

Example

CSP($\mathbb{Q}; <$) and CSP($\mathbb{N}; \neq$) are tractable (!).

Well studied ω-categorical algebras also include:

- Groups (Rosenstein, Felgner, Apps,...),
- Rings (Baldwin, Rose,...),
- Semigroups (my PhD,...),
- Boolean algebras (classified - finitely many atoms),
- Fields (must be finite).

Part 3: The power of polymorphisms

Polymorphisms

- The hardness of a problem often comes from a lack of symmetry.
- Our usual objects that capture symmetry (automorphism group or endomorphism monoid) are not sufficient.
- We require a more general symmetry - polymorphisms!

Definition

A **polymorphism** of a structure M is an n-ary homomorphism $f : M^n \to M$. The set of all polymorphisms of M is denoted $\mathrm{Pol}(M)$.

For any structure M, the set $\mathrm{Pol}(M)$ forms a *clone* i.e. is closed under composition and contains the projections.

Polymorphisms of $(\mathcal{A}; \neq)$

Lemma

Let $\mathcal{A} = (A; F)$ be an algebra. Then $f : A^n \to A$ is a polymorphism of $(\mathcal{A}, \neq)$ if and only if f is an algebra homomorphism and

$$x_1 \neq y_1, \ldots, x_n \neq y_n \Rightarrow f(x_1, \ldots, x_n) \neq f(y_1, \ldots, y_n)$$

or, equivalently, if

$$f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n) \Rightarrow x_i = y_i \text{ for some } 1 \leq i \leq n.$$

In particular, every endomorphism of $(\mathcal{A}, \neq)$ is an embedding.
i.e. $\mathcal{A}$ is a core.

Hence if $\mathcal{A}$ and $\mathcal{B}$ are ω-categorical then CSP$(\mathcal{A}, \neq)$=CSP$(\mathcal{B}, \neq)$ if and only if A and B are *bi-embeddable* i.e. $A \hookrightarrow B$ and $B \hookrightarrow A$.

We can thus work up to bi-embeddablity!

Siggers vs pseudo-Siggers

Definition

A 6-ary operation $f \in \mathrm{Pol}(\mathcal{A})$ is called a **Siggers** polymorphism if

$$f(x, y, x, z, y, z) \approx f(y, x, z, x, z, y).$$

For finite CSPs, the existence of a *Siggers* polymorphism is necessary and sufficient for tractability (Bulatov, Zhuk 2017).
For infinite structures this is no longer true...We need greater generality!

Definition

A 6-ary operation $f \in \mathrm{Pol}(\mathcal{A})$ is called a **pseudo-Siggers** polymorphism if

$$\alpha f(x, y, x, z, y, z) \approx \beta f(y, x, z, x, z, y)$$

for some unary operations $\alpha, \beta \in \mathrm{Pol}(\mathcal{A})$.

Model-complete

We call a structure M **model-complete** if every first-order sentence is equivalent to an existential sentence over M.

Theorem (Bodirsky, 07')

Every ω-categorical structure is homomorphically equivalent to a model-complete core, which is unique and ω-categorical.

Corollary

Let $\mathcal{A}$ be an ω-categorical algebra. Then there exists a unique ω-categorical algebra $\mathcal{B}$ which is bi-embeddable with $\mathcal{A}$ and with $(\mathcal{B}, \neq)$ model-complete.

Example

The abelian groups $\mathbb{Z}_2 \oplus \mathbb{Z}_4^{(\omega)}$ and $\mathbb{Z}_4^{(\omega)}$ are bi-embeddable, and $(\mathbb{Z}_4^{(\omega)}, \neq)$ is model-complete.

The pseudo-Siggers theorem

Let $\mathscr{P}$ denote the clone of projections on a two-element set.

Theorem (Barto, Pinsker 06')

Let M be an ω-categorical structure which is a model-complete core. Then at least one of the following holds.

- *M has a pseudo-Siggers polymorphism.*
- *M Pol(M) is "small" (has a uniformly continuous minor-preserving map to $\mathscr{P}$); in this case, CSP(M) is NP-hard.*

However, the two possibilities in the theorem are not mutually exclusive.

If $\mathbb{A}$ is the atomless Boolean algebra then $(\mathbb{A}; \neq)$ has a pseudo-Siggers polymorphism, but $\text{Pol}(\mathbb{A}, \neq)$ has a u.c. minor-preserving map to $\mathscr{P}$.

Aim

Show that a dichotomy exists for both abelian groups and semilattices; Either $(A; \neq)$ has a pseudo-Siggers polymorphism, or Pol($A; \neq$) has a u.c. minor-preserving map to $\mathscr{P}$.

Part 4: Groups

Groups

- Given an ω-categorical algebra $\mathcal{A}$, if f is a pseudo-Siggers operation of $(\mathcal{A}, \neq)$ then for all $x, y, z, u, v, w \in A$

$$
\begin{aligned}
& f(x,y,x,z,y,z) = f(u,v,u,w,v,w) \qquad \text{(Property 1)} \\
\Leftrightarrow \quad & f(y,x,z,x,z,y) = f(v,u,w,u,w,v).
\end{aligned}
$$

- Let G be a group with identity 1 and $f \in Pol(G; \neq)$. Then

$$f(x_1, \ldots, x_n) = f(x_1, 1, 1, \ldots, 1) f(1, x_2, 1, \ldots, 1) \cdots f(1, 1, \ldots, 1, x_n).$$

- This, together with Property (1) shows that if $(G; \neq)$ has a pseudo-Siggers polymorphism then it is 'close' to being bi-embeddable with $G \times G$.

Groups

Proposition (Bodirsky, TQG)

Let G be an ω-categorical group such that $(G, \neq)$ has a pseudo-Siggers polymorphism. Then at least one of the following holds.

- *G is bi-embeddable with $G \times G$.*
- *G is bi-embeddable with $G \times (G/\langle x \rangle)$ for some $x \in G$ of order 2.*

Rough proof.

One of the maps $x \mapsto f(x, 1, x, 1, 1, 1)$ and $x \mapsto f(1, x, 1, x, x, x)$ is injective as f preserves $\neq$:

$$f(1, x, 1, x, x, x) = 1 = f(y, x, y, x, x, x) \Rightarrow f(y, x, y, x, x, x) = 1.$$

Similarly, their images are disjoint. For $y \neq 1$, use Property (1):

$$f(1, y, 1, y, y, y) = 1 = f(1, 1, 1, 1, 1, 1) \Rightarrow f(y, 1, y, 1, y, y) = 1.$$

Hence $f(y, y, y, y, y^2, y^2) = 1 = f(1, 1, 1, 1, 1, 1)$, so $y^2 = 1$ etc... □

Abelian groups

Theorem

Every abelian group of finite exponent is a direct sum of cyclic groups $\mathbb{Z}_n$.

It is then a relatively simple exercise to find those which satisfy the necessary condition to having a pseudo-Siggers:

Proposition (Bodirsky, TQG)

Let G be an abelian group of finite exponent. Then $(G, \neq)$ has a pseudo-Siggers polymorphism if and only if G is bi-embeddable with $\mathbb{Z}_m^{(\omega)}$ or with $\mathbb{Z}_m^{(\omega)} \oplus \mathbb{Z}_{2m}$ for some $m \geq 1$.

Abelian groups

Theorem (Bodirsky, TQG)

Let G be an ω-categorical abelian group. Then the following are equivalent:

(i) *$Pol(G, \neq)$ has no u.c. minor-preserving map to $\mathscr{P}$,*

(ii) *$(G, \neq)$ has a pseudo-Siggers polymorphism,*

(iii) *G is bi-embeddable with $\mathbb{Z}_m^{(\omega)}$ or with $\mathbb{Z}_m^{(\omega)} \oplus \mathbb{Z}_{2m}$ for some $m \geq 1$.*

Moreover, in this case $CSP(G, \neq)$ is in P, and is NP-hard otherwise.

Key: If M is an ω-categorical structure with both a pseudo-Siggers polymorphism and with $\mathrm{Pol}(M)$ having a u.c. minor-preserving map to $\mathscr{P}$, then M is not ω-stable.

General groups

The non-abelian case remains open.

In particular, we have no example of an ω-categorical non-abelian group G with $\mathrm{CSP}(G; \neq)$ in P.

Theorem (Sarcino, Wood 1982)

There are 2^ω distinct (up to isomorphism) ω-categorical groups which are pairwise non bi-embeddable.

$\Rightarrow \exists$ ω-categorical groups G such that $\mathrm{CSP}(G; \neq)$ is undecidable.

Part 5: Semilattices

Semilattices

- A **semilattice** is an algebra $(Y; \wedge)$ where $\wedge$ is an associative, commutative, and idempotent binary operation.
- There exists a unique ω-categorical semilattice which embeds all finite semilattices and is **homogeneous**. We call this the *universal semilattice*, denoted $\mathbb{U}$.
- $\mathbb{U}$ is bi-embeddable with the meet-reduct of the atomless boolean algebra $(\mathbb{A}; \wedge, \vee, \neg, 0, 1)$.

Lemma (Bodirsky, TQG)

CSP$(\mathbb{U}; \neq)$ is tractable.

While semilattices do not necessarily possess an identity, property (1) still proves to be useful for proving hardness of CSP$(Y; \neq)$.

$$\begin{aligned} & f(x,y,x,z,y,z) = f(u,v,u,w,v,w) \qquad \text{(Property 1)} \\ \Leftrightarrow \quad & f(y,x,z,x,z,y) = f(v,u,w,u,w,v). \end{aligned}$$

Semilattices

Theorem (Bodirsky, TQG)

Let Y be a non-trivial ω-categorical semilattice. Then CSP$(Y; \neq)$ is tractable if Y is bi-embeddable with $\mathbb{U}$, and is NP-hard otherwise.

Proof idea:

- Y is bi-embeddable with $\mathbb{U}$ if and only if it embeds all finite Boolean algebras $(\mathbb{P}_n; \wedge)$.
- Show that every $\mathbb{P}_n$ embeds into Y if CSP$(Y; \neq)$ is not NP-hard.
- Use induction: true for $n = 2$ (since CSP$(Y, \neq)$ is NP-hard for $Y = (\mathbb{Q}; \min)$ - Bodirsky '09).
- Induction step: Use the existence of a pseudo-Siggers polymorphism.

□

Dichotomy

Theorem (Bodirsky, TQG)

Let Y be a countable ω-categorical semilattice. Then either

(i) *there is a u.c. minor-preserving map from Pol(Y; $\neq$) to $\mathscr{P}$, in which case CSP($Y, \neq$) is NP-hard, or*

(ii) *the model-complete core of $(Y, \neq)$ is isomorphic to $(\mathbb{U}, \neq)$, in which case CSP($Y, \neq$) is in P.*

Proof.

The following (height one) identities, discovered by Jakub Rydval, are preserved by all minor-preserving maps and are not satisfied by $\mathscr{P}$:
There are $f, g_1, \ldots, g_4 \in \mathrm{Pol}(\mathbb{U}, \neq)$ such that for all $x, y \in \mathbb{U}$

$$\begin{array}{ll} g_1(y,x,x) = f(x,y,x,x), & g_2(y,x,x) = f(y,x,x,x), \\ g_1(x,y,x) = f(x,x,y,x), & g_2(x,y,x) = f(x,x,y,x), \ \textit{etc} \\ g_1(x,x,y) = f(x,x,x,y), & g_2(x,x,y) = f(x,x,x,y), \end{array}$$

□

Lattices

Similar occurrences holds for lattices:

- An ω-categorical lattice L in which $(L; \neq)$ has a pseudo-Siggers polymorphism is bi-embeddable with $L \times L$.
- If L is distributive then $\mathrm{CSP}(L; \neq)$ is NP-hard.
- However: the universal lattice (which embeds all finite lattices) is not ω-categorical.

Open: Let L be a non-distributive ω-categorical lattice which is bi-embeddable with $L \times L$. What is the computational complexity of $\mathrm{CSP}(L; \neq)$?

Key: Can we classify the ω-categorical (model-complete) lattices L such that L is bi-embeddable with $L \times L$?