Complexity of Solving Promise Systems of Equations Over Algebras

Nick Jamesson
BLAST 2025

May 20, 2025

Constraint Satisfaction Problems (CSP)

Let $\mathbb{A} = (A; R_1^{\mathbb{A}}, \ldots, R_n^{\mathbb{A}})$ be a relational structure.

Example

$K_3 = (\{1, 2, 3\}; E_3)$ where
$E_3 = \{(1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2)\}$ the complete graph on three vertices.

Constraint Satisfaction Problems (CSP)

Let $\mathbb{A} = (A; R_1^{\mathbb{A}}, \dots, R_n^{\mathbb{A}})$ be a relational structure.

Example

$K_3 = (\{1, 2, 3\}; E_3)$ where
$E_3 = \{(1,2), (2,1), (1,3), (3,1), (2,3), (3,2)\}$ the complete graph on three vertices.

$\mathrm{CSP}(\mathbb{A})$

Input:	List of constraints in the signature of $\mathbb{A}$ $R_1(x, x, y)$ $R_2(x, y, z)$ $\dots$
Problem:	Is there an assignment of variables to elements of A such that each constraint holds in $\mathbb{A}$?

Constraint Satisfaction Problems (CSP)

Let $\mathbb{A} = (A; R_1^{\mathbb{A}}, \ldots, R_n^{\mathbb{A}})$ be a relational structure.

Example

$K_3 = (\{1,2,3\}; E_3)$ where
$E_3 = \{(1,2),(2,1),(1,3),(3,1),(2,3),(3,2)\}$ the complete graph on three vertices.

$\mathrm{CSP}(\mathbb{A})$

Input:	List of constraints in the signature of $\mathbb{A}$ $R_1(x,x,y)$ $R_2(x,y,z)$ $\ldots$
Problem:	Is there an assignment of variables to elements of A such that each constraint holds in $\mathbb{A}$?

Example

$\mathrm{CSP}(K_3)$: is a given graph 3-colorable?

Promise Constraint Satisfaction Problems (PCSP)

Let $\mathbb{A} = (A; R_1^{\mathbb{A}}, \ldots, R_n^{\mathbb{A}})$ and $\mathbb{B} = (B; R_1^{\mathbb{B}}, \ldots, R_n^{\mathbb{B}})$ with a homomorphism $\mathbb{A} \to \mathbb{B}$.

$\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$

Input: List of constraints in the signature of $\mathbb{A}$ and $\mathbb{B}$.

$R_1(x, x, y)$

$R_2(x, y, z)$

$\ldots$

Problem: Is there an assignment of variables to elements of A such that each constraint holds in $\mathbb{A}$, or not even such an assignment in $\mathbb{B}$?

Promise Constraint Satisfaction Problems (PCSP)

Let $\mathbb{A} = (A; R_1^{\mathbb{A}}, \ldots, R_n^{\mathbb{A}})$ and $\mathbb{B} = (B; R_1^{\mathbb{B}}, \ldots, R_n^{\mathbb{B}})$ with a homomorphism $\mathbb{A} \to \mathbb{B}$.

$\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$

Input:	List of constraints in the signature of $\mathbb{A}$ and $\mathbb{B}$. $R_1(x, x, y)$ $R_2(x, y, z)$ $\ldots$
Problem:	Is there an assignment of variables to elements of A such that each constraint holds in $\mathbb{A}$, or not even such an assignment in $\mathbb{B}$?

Example

$\mathrm{PCSP}(K_3, K_5)$: is a given graph is 3-colorable, or not even 5-colorable?

The promise in promise constraint satisfaction

- The promise in $\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$ is that every instance I does in fact have either a solution in $\mathbb{A}$ (a YES instance) or no solution in $\mathbb{B}$ (a NO instance).

The promise in promise constraint satisfaction

- The promise in $\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$ is that every instance I does in fact have either a solution in $\mathbb{A}$ (a YES instance) or no solution in $\mathbb{B}$ (a NO instance).
- The existence of a homomorphism $\mathbb{A} \to \mathbb{B}$ guarantees an instance cannot be both a YES instance and a NO instance.

Promise systems of equations

Let $\mathbf{A} = (A; f_1^{\mathbf{A}}, \ldots, f_n^{\mathbf{A}})$ and $\mathbf{B} = (B; f_1^{\mathbf{B}}, \ldots, f_n^{\mathbf{B}})$ with a homomorphism $\mathbf{A} \to \mathbf{B}$.

$\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$

Input: System of equations in the signature of $\mathbf{A}$ and $\mathbf{B}$

$f_1(x, y, , y) = f_1(f_2(x), z, y)$

$f_5(z, z) = f_2(y)$

$\ldots$

Problem: Is there a solution to the system in $\mathbf{A}$, or not even a solution in $\mathbf{B}$?

Larrauri and Živný (2024) initiated the study of promise systems of equations with promise systems of equations over semigroups.

Use of PCSP results

Theorem (Larose, Zádori 2006)

Let $\mathbf{A} = (A; f_1^{\mathbf{A}}, \dots, f_n^{\mathbf{A}})$. For a function f, let f° be its graph relation. Let $\mathbb{A}^\circ$ be the relational structure with domain A and with relations f_i° for all $f \in \{f_1^{\mathbf{A}}, \dots, f_n^{\mathbf{A}}\} \cup \{id\} \cup A$.

Then $\mathrm{SysPol}(\mathbf{A})$ is the log space equivalent to $\mathrm{CSP}(\mathbb{A}^\circ)$.

The same argument can be used to restate a promise system of equations as a PCSP.

Problem

What is the computational complexity of solving $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$?

Problem

What is the computational complexity of solving $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$?

- We assume all structures are finite with finite signature in the following.

Problem

What is the computational complexity of solving $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$?

- We assume all structures are finite with finite signature in the following.
- $\mathrm{SysTerm}(\mathbf{A}) = \mathrm{PEqn}(\mathbf{A}, \mathbf{A})$ is either in P or is NP-complete by CSP dichotomy (Bulatov 2017, Zhuk 2017).

Problem

What is the computational complexity of solving $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$?

- We assume all structures are finite with finite signature in the following.
- $\mathrm{SysTerm}(\mathbf{A}) = \mathrm{PEqn}(\mathbf{A}, \mathbf{A})$ is either in P or is NP-complete by CSP dichotomy (Bulatov 2017, Zhuk 2017).
- For all known examples, $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$ is either in P or is NP-hard.

Problem

What is the computational complexity of solving $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$?

- We assume all structures are finite with finite signature in the following.
- $\mathrm{SysTerm}(\mathbf{A}) = \mathrm{PEqn}(\mathbf{A}, \mathbf{A})$ is either in P or is NP-complete by CSP dichotomy (Bulatov 2017, Zhuk 2017).
- For all known examples, $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$ is either in P or is NP-hard.
- For tractability, one technique is to find a tractable sandwich. That is, find an algebra $\mathbf{C}$ such that there are homomorphisms $\mathbf{A} \to \mathbf{C} \to \mathbf{B}$ and $\mathrm{SysTerm}(\mathbf{C})$ is in P. Note that $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$ reduces to $\mathrm{SysTerm}(\mathbf{C}) = \mathrm{PEqn}(\mathbf{C}, \mathbf{C})$.

Problem

What is the computational complexity of solving $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$?

- We assume all structures are finite with finite signature in the following.
- $\mathrm{SysTerm}(\mathbf{A}) = \mathrm{PEqn}(\mathbf{A}, \mathbf{A})$ is either in P or is NP-complete by CSP dichotomy (Bulatov 2017, Zhuk 2017).
- For all known examples, $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$ is either in P or is NP-hard.
- For tractability, one technique is to find a tractable sandwich. That is, find an algebra $\mathbf{C}$ such that there are homomorphisms $\mathbf{A} \to \mathbf{C} \to \mathbf{B}$ and $\mathrm{SysTerm}(\mathbf{C})$ is in P. Note that $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$ reduces to $\mathrm{SysTerm}(\mathbf{C}) = \mathrm{PEqn}(\mathbf{C}, \mathbf{C})$.
- For hardness, we need to show the set of polymorphisms from an algebra $\mathbf{A}$ to an algebra $\mathbf{B}$ is not sufficiently rich.

Polymorphisms

Definition

Let $\mathbf{A}$ and $\mathbf{B}$ be algebras of the same signature. A *polymorphism* p from $\mathbf{A}$ to $\mathbf{B}$ is a homomorphism $p\colon \mathbf{A}^n \to \mathbf{B}$ for some $n \in \mathbb{N}$.
$\mathrm{Pol}(\mathbf{A}, \mathbf{B}) :=$ the set of polymorphisms from $\mathbf{A}$ to $\mathbf{B}$.

Polymorphisms

Definition

Let $\mathbf{A}$ and $\mathbf{B}$ be algebras of the same signature. A *polymorphism* p from $\mathbf{A}$ to $\mathbf{B}$ is a homomorphism $p\colon \mathbf{A}^n \to \mathbf{B}$ for some $n \in \mathbb{N}$.
$\mathrm{Pol}(\mathbf{A}, \mathbf{B}) :=$ the set of polymorphisms from $\mathbf{A}$ to $\mathbf{B}$.

1. $\mathrm{Pol}(\mathbf{A}, \mathbf{A})$ determines the complexity of $\mathrm{SysTerm}(\mathbf{A})$.

Polymorphisms

Definition

Let $\mathbf{A}$ and $\mathbf{B}$ be algebras of the same signature. A *polymorphism* p from $\mathbf{A}$ to $\mathbf{B}$ is a homomorphism $p \colon \mathbf{A}^n \to \mathbf{B}$ for some $n \in \mathbb{N}$.
$\mathrm{Pol}(\mathbf{A}, \mathbf{B}) :=$ the set of polymorphisms from $\mathbf{A}$ to $\mathbf{B}$.

1. $\mathrm{Pol}(\mathbf{A}, \mathbf{A})$ determines the complexity of $\mathrm{SysTerm}(\mathbf{A})$.
2. Similarly $\mathrm{Pol}(\mathbf{A}, \mathbf{B})$ determines the complexity of $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$.

First complexity result

For monoids, Larrauri and Živný proved the following:

Theorem (Larrauri, Živný 2024)

Let $\mathbf{A}$ and $\mathbf{B}$ be monoids possibly with additional constant (0-ary) operations with a homomorphism $\mathbf{A} \to \mathbf{B}$.

If there exists $\psi : \mathbf{A} \to \mathbf{B}$ such that $\psi(\mathbf{A})$ is commutative and a union of subgroups, then $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$ is in P.

Otherwise $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$ is NP-hard.

Extending the results for monoids

Theorem (NJ 2025)

Let $\mathbf{A}$ and $\mathbf{B}$ be algebras with a homomorphism $\mathbf{A} \to \mathbf{B}$.

Let $\overline{\mathbf{A}}$ be the reduct of $\mathbf{A}$ without constants.

Let $e \in A$ be such that $\{e\} \leq \overline{\mathbf{A}}$.

Let m be a term of $\overline{\mathbf{A}}$ such that $m^{\mathbf{A}}(x, e, e) = x = m^{\mathbf{A}}(e, e, x)$ for all $x \in A$.

If there is a homomorphism $\psi\colon \mathbf{A} \to \mathbf{B}$ such that:

Extending the results for monoids

Theorem (NJ 2025)

Let $\mathbf{A}$ and $\mathbf{B}$ be algebras with a homomorphism $\mathbf{A} \to \mathbf{B}$.

Let $\overline{\mathbf{A}}$ be the reduct of $\mathbf{A}$ without constants.

Let $e \in A$ be such that $\{e\} \leq \overline{\mathbf{A}}$.

Let m be a term of $\overline{\mathbf{A}}$ such that $m^{\mathbf{A}}(x, e, e) = x = m^{\mathbf{A}}(e, e, x)$ for all $x \in A$.

If there is a homomorphism $\psi\colon \mathbf{A} \to \mathbf{B}$ such that:

1. $m^{\psi(\mathbf{A})}(x, \psi(e), y)$ is a polymorphism of $\psi(\overline{\mathbf{A}})$

Extending the results for monoids

Theorem (NJ 2025)

Let $\mathbf{A}$ and $\mathbf{B}$ be algebras with a homomorphism $\mathbf{A} \to \mathbf{B}$.

Let $\overline{\mathbf{A}}$ be the reduct of $\mathbf{A}$ without constants.

Let $e \in A$ be such that $\{e\} \leq \overline{\mathbf{A}}$.

Let m be a term of $\overline{\mathbf{A}}$ such that $m^{\mathbf{A}}(x, e, e) = x = m^{\mathbf{A}}(e, e, x)$ for all $x \in A$.

If there is a homomorphism $\psi \colon \mathbf{A} \to \mathbf{B}$ such that:

1. $m^{\psi(\mathbf{A})}(x, \psi(e), y)$ is a polymorphism of $\psi(\overline{\mathbf{A}})$
2. $(\psi(A); m^{\psi(\mathbf{A})}(x, \psi(e), y))$ is a union of subgroups

Extending the results for monoids

Theorem (NJ 2025)

Let $\mathbf{A}$ and $\mathbf{B}$ be algebras with a homomorphism $\mathbf{A} \to \mathbf{B}$.

Let $\overline{\mathbf{A}}$ be the reduct of $\mathbf{A}$ without constants.

Let $e \in A$ be such that $\{e\} \leq \overline{\mathbf{A}}$.

Let m be a term of $\overline{\mathbf{A}}$ such that $m^{\mathbf{A}}(x, e, e) = x = m^{\mathbf{A}}(e, e, x)$ for all $x \in A$.

If there is a homomorphism $\psi\colon \mathbf{A} \to \mathbf{B}$ such that:

1. $m^{\psi(\mathbf{A})}(x, \psi(e), y)$ is a polymorphism of $\psi(\overline{\mathbf{A}})$
2. $(\psi(A); m^{\psi(\mathbf{A})}(x, \psi(e), y))$ is a union of subgroups

Extending the results for monoids

Theorem (NJ 2025)

Let $\mathbf{A}$ and $\mathbf{B}$ be algebras with a homomorphism $\mathbf{A} \to \mathbf{B}$.

Let $\overline{\mathbf{A}}$ be the reduct of $\mathbf{A}$ without constants.

Let $e \in A$ be such that $\{e\} \leq \overline{\mathbf{A}}$.

Let m be a term of $\overline{\mathbf{A}}$ such that $m^{\mathbf{A}}(x, e, e) = x = m^{\mathbf{A}}(e, e, x)$ for all $x \in A$.

If there is a homomorphism $\psi \colon \mathbf{A} \to \mathbf{B}$ such that:

1. $m^{\psi(\mathbf{A})}(x, \psi(e), y)$ is a polymorphism of $\psi(\overline{\mathbf{A}})$
2. $(\psi(A); m^{\psi(\mathbf{A})}(x, \psi(e), y))$ is a union of subgroups

then $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$ is in P. Otherwise $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$ is NP-hard.

Mal'cev algebras

Definition

A *Mal'cev algebra* $\mathbf{A}$ is an algebra with a term m satisfying the identity $m^{\mathbf{A}}(x, x, y) = y = m^{\mathbf{A}}(y, x, x)$.

Mal'cev algebras

Definition

A *Mal'cev algebra* $\mathbf{A}$ is an algebra with a term m satisfying the identity $m^{\mathbf{A}}(x,x,y) = y = m^{\mathbf{A}}(y,x,x)$.

Example

A group is a Mal'cev algebra with Mal'cev term $m(x,y,z) = xy^{-1}z$.

Mal'cev algebras

Definition

A *Mal'cev algebra* $\mathbf{A}$ is an algebra with a term m satisfying the identity $m^{\mathbf{A}}(x, x, y) = y = m^{\mathbf{A}}(y, x, x)$.

Example

A group is a Mal'cev algebra with Mal'cev term $m(x, y, z) = xy^{-1}z$.

Theorem (NJ 2025)

Let $\mathbf{A}$, $\mathbf{B}$ be Mal'cev algebras with a homomorphism $\mathbf{A} \to \mathbf{B}$ and with at least one constant symbol in their signature.

If there is a homomorphism $\psi : \mathbf{A} \to \mathbf{B}$ such that $\psi(\mathbf{A})$ is abelian, then $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$ is in P. Otherwise $\mathrm{PEqn}(\mathbf{A}, \mathbf{B})$ is NP-hard.

Function Minions

In general, polymorphisms from $\mathrm{Pol}(\mathbf{A}, \mathbf{B})$ cannot be composed. So although $\mathrm{Pol}(\mathbf{A}, \mathbf{B})$ is not a clone (as $\mathrm{Pol}(\mathbf{A}, \mathbf{A})$ is), it is a *minion*.

Definition

For $g\colon A^m \to B$ and $\pi\colon [m] \to [n]$, we call

$$g^{(\pi)}(x_1, \ldots, \ldots x_n) := g(x_{\pi(1)}, \ldots x_{\pi(m)})$$

a *minor* of g.

Function Minions

In general, polymorphisms from $\mathrm{Pol}(\mathbf{A}, \mathbf{B})$ cannot be composed. So although $\mathrm{Pol}(\mathbf{A}, \mathbf{B})$ is not a clone (as $\mathrm{Pol}(\mathbf{A}, \mathbf{A})$ is), it is a *minion*.

Definition

For $g \colon A^m \to B$ and $\pi \colon [m] \to [n]$, we call

$$g^{(\pi)}(x_1, \ldots, \ldots x_n) := g(x_{\pi(1)}, \ldots x_{\pi(m)})$$

a *minor* of g.

Definition

$\mathcal{M} \subseteq \{f \colon A^n \to B : n \geq 1\}$ is a *minion* from A to B if $\mathcal{M}$ is closed under taking minors.

A tool for proving hardness

Barto et al. (2021) describe several techniques for proving NP-hardness of a PCSP. The previous results use the following:

Definition

Let $\mathcal{M}$ be a minion. Suppose there is a constant K and a function I which for all $m, n > 0$ satisfies:

A tool for proving hardness

Barto et al. (2021) describe several techniques for proving NP-hardness of a PCSP. The previous results use the following:

Definition

Let $\mathcal{M}$ be a minion. Suppose there is a constant K and a function I which for all $m, n > 0$ satisfies:

1. For each $p \in \mathcal{M}^{(n)}$, we have $I(p) \subseteq [n]$ satisfying $|I(p)| < K$

A tool for proving hardness

Barto et al. (2021) describe several techniques for proving NP-hardness of a PCSP. The previous results use the following:

Definition

Let $\mathcal{M}$ be a minion. Suppose there is a constant K and a function I which for all $m, n > 0$ satisfies:

1. For each $p \in \mathcal{M}^{(n)}$, we have $I(p) \subseteq [n]$ satisfying $|I(p)| < K$
2. For each $\pi : [m] \to [n]$ and $q \in \mathcal{M}^{(m)}$, we have $\pi(I(q)) \cap I(q^{(\pi)}) \neq \emptyset$.

A tool for proving hardness

Barto et al. (2021) describe several techniques for proving NP-hardness of a PCSP. The previous results use the following:

Definition

Let $\mathcal{M}$ be a minion. Suppose there is a constant K and a function I which for all $m, n > 0$ satisfies:

1. For each $p \in \mathcal{M}^{(n)}$, we have $I(p) \subseteq [n]$ satisfying $|I(p)| < K$
2. For each $\pi : [m] \to [n]$ and $q \in \mathcal{M}^{(m)}$, we have $\pi(I(q)) \cap I(q^{(\pi)}) \neq \emptyset$.

A tool for proving hardness

Barto et al. (2021) describe several techniques for proving NP-hardness of a PCSP. The previous results use the following:

Definition

Let $\mathcal{M}$ be a minion. Suppose there is a constant K and a function I which for all $m, n > 0$ satisfies:

1. For each $p \in \mathcal{M}^{(n)}$, we have $I(p) \subseteq [n]$ satisfying $|I(p)| < K$
2. For each $\pi : [m] \to [n]$ and $q \in \mathcal{M}^{(m)}$, we have $\pi(I(q)) \cap I(q^{(\pi)}) \neq \emptyset$.

Then I is a *selection function* for $\mathcal{M}$ with bound K.

A tool for proving hardness

Theorem (Barto et al. 2021)

Let $\mathbb{A}$ and $\mathbb{B}$ be relational structures with a homomorphism $\mathbb{A} \to \mathbb{B}$. Let $\mathcal{M} = \mathrm{Pol}(\mathbb{A}, \mathbb{B})$. If there exists a selection function I with bound K for $\mathcal{M}$, then $\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$ is NP-hard.

References

Libor Barto, Jakub Bulín, Andrei Krokhin, and Jakub Opršal.
Algebraic approach to promise constraint satisfaction.
J. ACM, 68(4):Art. 28, 66, 2021.

References

Libor Barto, Jakub Bulín, Andrei Krokhin, and Jakub Opršal.
Algebraic approach to promise constraint satisfaction.
J. ACM, 68(4):Art. 28, 66, 2021.

Benoit Larose and László Zádori.
Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras.
Internat. J. Algebra Comput., 16(3):563–581, 2006.

References

Libor Barto, Jakub Bulín, Andrei Krokhin, and Jakub Opršal.
Algebraic approach to promise constraint satisfaction.
J. ACM, 68(4):Art. 28, 66, 2021.

Benoit Larose and László Zádori.
Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras.
Internat. J. Algebra Comput., 16(3):563–581, 2006.

Alberto Larrauri and Stanislav Živný.
Solving promise equations over monoids and groups.
https://arxiv.org/abs/2402.08434, 2024.