Finite Simple Groups in the Primitive Positive Constructability Poset

Sebastian Meyer, joint work with Florian Starke

Institute of Algebra
TU Dresden

8th October 2024

European Research Council
Established by the European Commission

ERC Synergy Grant POCOCOP (GA 101071674)

The Primitive Positive Constructability Poset

The Primitive Positive Constructability Poset

Structures

Definition

A *(relational) structure* $\underline{A}$ over a signature σ is a set A together with subsets of powers of A for each element in σ.

Examples

Structures

Definition

A *(relational) structure* $\underline{A}$ over a signature σ is a set A together with subsets of powers of A for each element in σ.

Examples of structures

- $(\mathbb{N};+,\cdot,1)$ where $+$ and $\cdot$ are considered as subset of $\mathbb{N}^3$ and 1 is considered as subset of $\mathbb{N}^1$.
- All groups, rings, modules,... in the usual way.
- A group action $G \curvearrowright X$ defines a structure on X, which we call $S(G \curvearrowright X)$. The signature is G and the relation corresponding to $g \in G$ is $\{(x, g.x) \mid x \in X\}$.
- graphs (with a binary relation)
- 3-SAT $= (\{\top,\bot\};\top,\bot,\wedge,\vee,\neg)$

Problems

Definition

The *constraint satisfaction problem* or CSP of a structure $\underline{A}$ is to decide whether a primitive positive formula (first order, no $\forall, \neg, \vee$) is true in this structure.

Examples

Problems

Definition

The *constraint satisfaction problem* or CSP of a structure $\underline{A}$ is to decide whether a primitive positive formula (first order, no $\forall, \neg, \vee$) is true in this structure.

Examples

- $\mathrm{CSP}(3\text{-SAT}) = \mathrm{CSP}(\{\top, \bot\}; \top, \bot, \wedge, \vee, \neg)$ is the usual 3-SAT problem (NP-complete)
- $\mathrm{CSP}(\mathbb{N}; +, \cdot, 1)$ decides whether a system of equations can be solved in $\mathbb{N}$. (Turing Complete)
- The CSP of a finite (undirected) graph is to decide whether another finite graph can be mapped to this one. (If the graph is bipartite, this is in P, else it is NP-complete. Hell, Nešetřil 1990)
- The CSP of a finite structure is in P or NP complete. (Bulatov 2017; Zhuk 2017)

Reductions

Definition

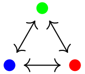
A *primitive positive construction* of a σ-structure $\underline{A}$ in a τ-structure $\underline{B}$ consists of

1. a positive integer n
2. a σ-structure $\underline{\tilde{B}}$ with base set B^n, where the k-ary relations of $\underline{\tilde{B}}$ are pp-definable as kn-ary relations in $\underline{B}$
3. σ-homomorphisms $f\colon \underline{\tilde{B}} \to \underline{A}$ and $g\colon \underline{A} \to \underline{\tilde{B}}$.

A primitive positive construction gives a logspace reduction from CSP($\underline{A}$) to CSP($\underline{B}$).

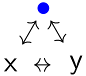
Example

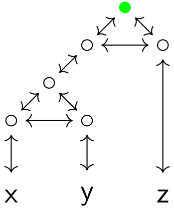
Graph 3-coloring (with colors ${\color{blue}\bullet}$, ${\color{red}\bullet}$, ${\color{green}\bullet}$) is NP-hard, because one can reduce

3-SAT to  by $n = 1$ and

$\top = {\color{green}\bullet}$

$\bot = {\color{red}\bullet}$

unequal(x, y) = 

$x \vee y \vee z$ = 

with identification maps

$$f({\color{red}\bullet}) = \bot \qquad g(\bot) = {\color{red}\bullet}$$

$$f({\color{blue}\bullet}) = f({\color{green}\bullet}) = \top \qquad g(\top) = {\color{green}\bullet}$$

Algebraically

Definition

A *polymorphism* of a σ-structure $\underline{A}$ is a homomorphism $\underline{A}^n \to \underline{A}$ for $n \in \mathbb{N}$.

$$\begin{array}{cccccc}
x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} & \overset{f}{\mapsto} & y_1 \\
x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} & \mapsto & y_2 \\
x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} & \mapsto & y_3 \\
\pitchfork & \pitchfork & \pitchfork & \pitchfork & \Longrightarrow & \pitchfork \\
R & R & R & R & & R
\end{array}$$

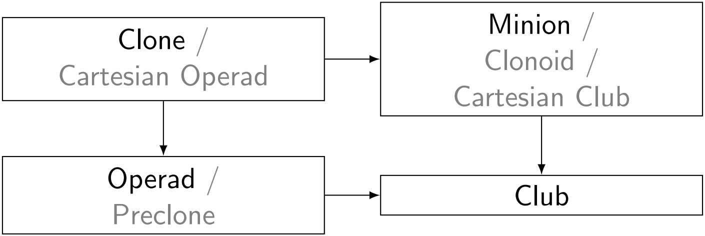
Algebraically

Definition

A *polymorphism* of a σ-structure $\underline{A}$ is a homomorphism $\underline{A}^n \to \underline{A}$ for $n \in \mathbb{N}$.

$$\begin{array}{cccccc} x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} & \overset{f}{\mapsto} & y_1 \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} & \mapsto & y_2 \\ x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} & \mapsto & y_3 \\ \pitchfork & \pitchfork & \pitchfork & \pitchfork & \Longrightarrow & \pitchfork \\ R & R & R & R & & R \end{array}$$

The set $\mathrm{Pol}(\underline{A})$ of all polymorphisms has the structure of a



Minions

The *minor* of $f\colon A^n \to A$ along $\alpha\colon [n] \to [m]$ is the map $f_\alpha\colon A^m \to A, (x_1, \ldots, x_m) \mapsto f(x_{\alpha(1)}, \ldots, x_{\alpha(n)})$.

Definition

A *minion homomorphism* from $\mathrm{Pol}(\underline{A})$ to $\mathrm{Pol}(\underline{B})$ is a map of sets F, that

- preserves arities and
- preserves minors, i.e. $F(f_\alpha) = (Ff)_\alpha$

Picture from https://www.pngwing.com/id/free-png-svred, at 7.Oct.2024

Minor Condition

A *height-1-condition* or *minor condition* of $\underline{A}$ is a condition of the form

$$\exists f \in \mathrm{Pol}(\underline{A}) : \bigwedge f_\alpha = f_\beta$$

Examples

$f(x) = f(y)$	constant
$f(x,x,x) = f(x,y,y) = f(y,y,x)$	quasi Maltsev
$f(x,x,x) = f(x,x,y) = f(x,y,x) = f(y,x,x)$	quasi majority
$f(x,y,z) = f(y,z,x) = f(y,x,z)$	(fully) symmetric of arity 3
$f(x,x,y) = f(x,y,y)$ and symmetric	totally symmetric of arity 3
$f(x,x,y) = f(z,z,y)$ and symmetric	general. minority of arity 3

Three Definitions

Theorem (Barto, Opršal, Pinsker 2018)

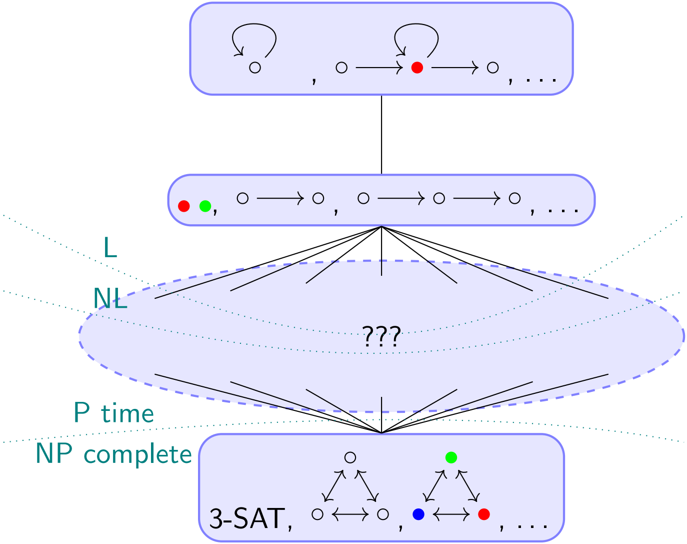
For two structures $\underline{A}$ and $\underline{B}$, the following is equivalent:

1. *$\underline{A}$ pp-constructs $\underline{B}$.*
2. *There is a minion-homomorphism* $\mathrm{Pol}(\underline{A}) \to \mathrm{Pol}(\underline{B})$.
3. *Every minor condition valid in* $\mathrm{Pol}(\underline{A})$ *is valid in* $\mathrm{Pol}(\underline{B})$.

In this case, $\mathrm{CSP}(\underline{B})$ reduces to $\mathrm{CSP}(\underline{A})$ in logspace (L).

The Primitive Positive Constructability Poset

The PP-Constructability Poset on Finite Structures



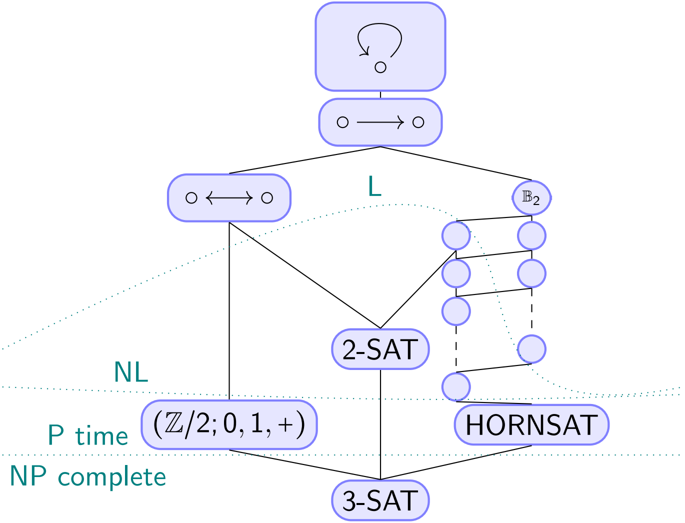
The PP-Constructability Poset on Finite Structures

1. Every equivalence class contains an idempotent structure $\underline{A}$.

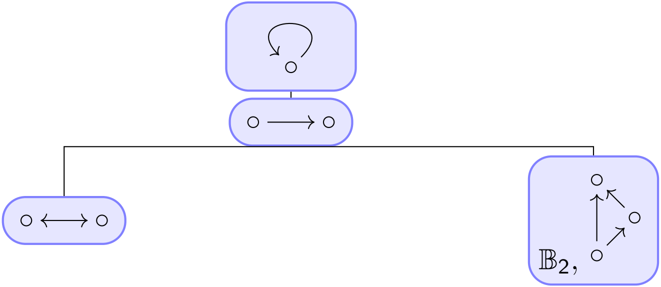
$$\mathrm{End}(\underline{A}) = \{\mathrm{id}_A\}$$

2. The poset of all smooth digraphs is classified (Bodirsky, Starke, Vucaj 2021)
3. The poset of all 2-Element structures is classified (Bodirsky, Vucaj 2020)

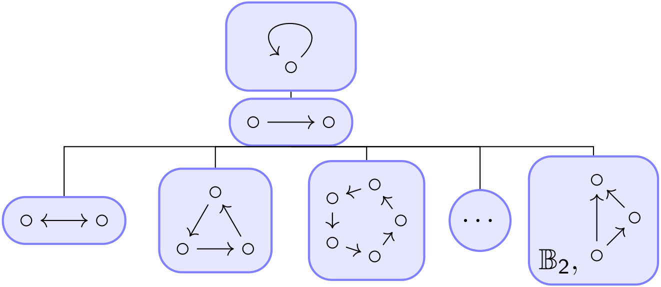
The PP-Constructability Poset on 2-Element Structures



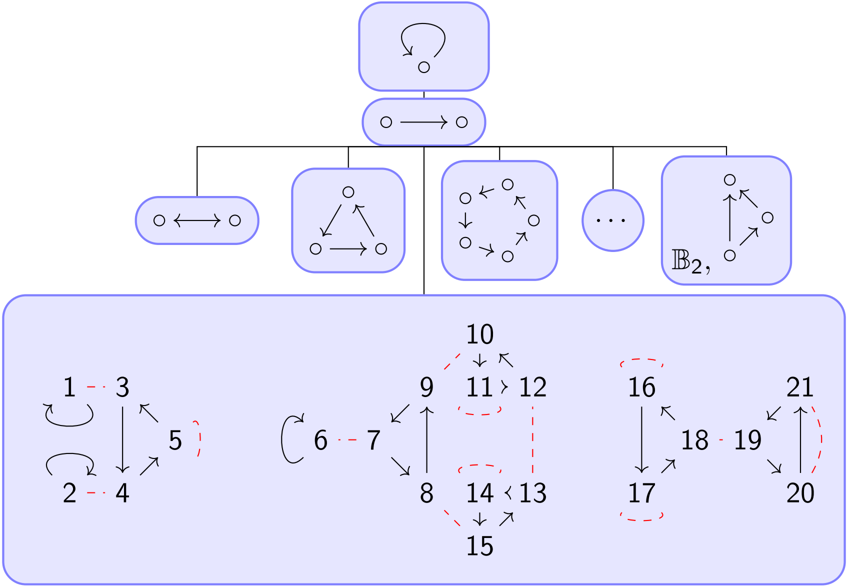
The Third Layer of the PP-Constructability Poset



The Third Layer of the PP-Constructability Poset



The Third Layer of the PP-Constructability Poset



The Third Layer of the PP-Constructability Poset

Theorem

The pp-constructabillity poset has a third layer consisting of the equivalence classes of

1. $\mathbb{B}_2$ *and*
2. *for all finite simple groups* G*, the structure* $S(G \curvearrowright \mathbb{P}(G))$*, where* $\mathbb{P}(G)$ *is the disjoint union of all primitive group actions.*

Moreover,

$$\mathbb{P}(G) = \begin{cases} G & \text{(with multiplication)} \\ & \text{if } G \text{ is cyclic} \\ \{M \leq G \text{ maximal subgroup}\} & \text{(with conjugation)} \\ & \text{if } G \text{ is nonabelian simple} \end{cases}$$

Proof overview

Let $\underline{A}$ be a structure.

1. If $\underline{A}$ has a quasi Maltsev polymorphism and fully symmetric polymorphisms of all arities, then $\circ \longrightarrow \circ$ pp-constructs $\underline{A}$.
2. If $\underline{A}$ has no quasi Maltsev polymorphism, then $\underline{A}$ pp-constructs $\mathbb{B}_2$. (Opršal 2018)
3. If $\underline{A}$ has not fully symmetric polymorphism of an arity n, then $\underline{A}$ pp-constructs $S(G \curvearrowright \mathbb{P}(G))$ for G finite simple group.
4. $S(G \curvearrowright \mathbb{P}(G))$ does not pp-construct $S(G' \curvearrowright \mathbb{P}(G'))$ for $G \neq G'$ different, finite simple

Part 1

Let $\underline{A}$ be a structure with $\mathrm{End}(\underline{A}) = \mathrm{id}_A$, quasi Maltsev, symetric of all arities.

$$f(x,x,x) = f(x,y,y) = f(y,y,x) = x \qquad \text{~~quasi~~ Maltsev}$$

$$f(x,y,z) = f(y,z,x) = f(y,x,z) \qquad \text{(fully) symmetric of arity 3}$$

Part 1

Let $\underline{A}$ be a structure with $\mathrm{End}(\underline{A}) = \mathrm{id}_A$, quasi Maltsev, symetric of all arities.

$$f(x,x,x) = f(x,y,y) = f(y,y,x) = x \qquad \text{~~quasi~~ Maltsev}$$

$$f(x,y,z) = f(y,z,x) = f(y,x,z) \qquad \text{(fully) symmetric of arity 3}$$

- $\underline{A}$ has a majority polymorphism. (Vucaj 2023)

$$x = f(x,x,x) = f(x,x,y) = f(x,y,x) = f(y,x,x) \qquad \text{~~quasi~~ majority}$$

Part 1

Let $\underline{A}$ be a structure with $\mathrm{End}(\underline{A}) = \mathrm{id}_A$, quasi Maltsev, symetric of all arities.

$$f(x,x,x) = f(x,y,y) = f(y,y,x) = x \qquad \text{~~quasi~~ Maltsev}$$

$$f(x,y,z) = f(y,z,x) = f(y,x,z) \qquad \text{(fully) symmetric of arity 3}$$

- $\underline{A}$ has a majority polymorphism. (Vucaj 2023)

$$x = f(x,x,x) = f(x,x,y) = f(x,y,x) = f(y,x,x) \quad \text{~~quasi~~ majority}$$

- $\underline{A}$ has generalised pairing polymorphisms: arity $2n+1$, mapping

$$\text{permutation of } (x, y_1, y_1, y_2, y_2, \dots, y_n, y_n) \mapsto x$$

Proof: Induction, Exercise. Hint:

$$\text{majority}\begin{pmatrix} \text{Maltsev}(x_1,x_3,x_2) \\ \text{Maltsev}(x_3,x_2,x_1) \\ \text{Maltsev}(x_2,x_1,x_3) \end{pmatrix}, \quad \text{Maltsev}(x_1, \text{pairing}(x_3,\dots,x_{2n+1}), x_2)$$

Part 1

- $\underline{A}$ has *symmetric* generalised pairing polymorphisms of arity n.

$$\text{symmetric}_{\text{arity } n!}(\text{pairing}(\text{permutation of}(x_1, \ldots, x_n)) \mid \text{all permutations})$$

Part 1

- $\underline{A}$ has *symmetric* generalised pairing polymorphisms of arity n.

$$\text{symmetric}_{\text{arity } n!}(\text{pairing}(\text{permutation of}(x_1, \ldots, x_n)) \mid \text{all permutations})$$

- $\underline{A}$ has generalised minority polymorphisms of arity n.

$$\text{sym. pair}_{\text{arity } 2^{n-1}-1}(\text{g. min}(A) \mid A \text{ odd proper subset of}(x_1, \ldots, x_n))$$

Part 1

- $\underline{A}$ has *symmetric* generalised pairing polymorphisms of arity n.

$$\text{symmetric}_{\text{arity } n!}(\text{pairing}(\text{permutation of}(x_1, \dots, x_n)) \mid \text{all permutations})$$

- $\underline{A}$ has generalised minority polymorphisms of arity n.

$$\text{sym. pair}_{\text{arity } 2^{n-1}-1}(\text{g. min}(A) \mid A \text{ odd proper subset of}(x_1, \dots, x_n))$$

- $\underline{A}$ has totally symmetric polymorphisms of arity n.

$$\text{symmetric}_{\text{arity } 2^{n-1}}(\text{g. min}(A) \mid A \text{ odd subset of}(x_1, \dots, x_n))$$

Part 1

- $\underline{A}$ has *symmetric* generalised pairing polymorphisms of arity n.

$$\text{symmetric}_{\text{arity } n!}(\text{pairing}(\text{permutation of}(x_1, \ldots, x_n)) \mid \text{all permutations})$$

- $\underline{A}$ has generalised minority polymorphisms of arity n.

$$\text{sym. pair}_{\text{arity } 2^{n-1}-1}(\text{g. min}(A) \mid A \text{ odd proper subset of}(x_1, \ldots, x_n))$$

- $\underline{A}$ has totally symmetric polymorphisms of arity n.

$$\text{symmetric}_{\text{arity } 2^{n-1}}(\text{g. min}(A) \mid A \text{ odd subset of}(x_1, \ldots, x_n))$$

- $\text{Pol}(\circ \longrightarrow \circ)$ maps to $\text{Pol}(\underline{A})$. (Vucaj, Zhuk 2024)
  Idea: Map the generators of $\text{Pol}(\circ \longrightarrow \circ)$ to generalized minority and totally symmetric polymorphism.

Part 3

If $\underline{A}$ has not fully symmetric polymorphism of an arity n, then $\underline{A}$ pp-constructs $S(G \curvearrowright \mathbb{P}(G))$ for G finite simple group.

Part 3

If $\underline{A}$ has not fully symmetric polymorphism of an arity n, then $\underline{A}$ pp-constructs $S(G \curvearrowright \mathbb{P}(G))$ for G finite simple group.

- Consider all polymorphisms $\underline{A}^n \to \underline{A}$.

Part 3

If $\underline{A}$ has not fully symmetric polymorphism of an arity n, then $\underline{A}$ pp-constructs $S(G \curvearrowright \mathbb{P}(G))$ for G finite simple group.

- Consider all polymorphisms $\underline{A}^n \to \underline{A}$.
- It is a subset $\mathrm{Pol}_n(\underline{A}) \subseteq A^{A^n}$.

Part 3

If $\underline{A}$ has not fully symmetric polymorphism of an arity n, then $\underline{A}$ pp-constructs $S(G \curvearrowright \mathbb{P}(G))$ for G finite simple group.

- Consider all polymorphisms $\underline{A}^n \to \underline{A}$.
- It is a subset $\mathrm{Pol}_n(\underline{A}) \subseteq A^{A^n}$.
- It is pp-definable.

Part 3

If $\underline{A}$ has not fully symmetric polymorphism of an arity n, then $\underline{A}$ pp-constructs $S(G \curvearrowright \mathbb{P}(G))$ for G finite simple group.

- Consider all polymorphisms $\underline{A}^n \to \underline{A}$.
- It is a subset $\mathrm{Pol}_n(\underline{A}) \subseteq A^{A^n}$.
- It is pp-definable.
- It has an action of $S_n = \mathrm{Sym}(n)$ by permuting entries.

Part 3

If $\underline{A}$ has not fully symmetric polymorphism of an arity n, then $\underline{A}$ pp-constructs $S(G \curvearrowright \mathbb{P}(G))$ for G finite simple group.

- Consider all polymorphisms $\underline{A}^n \to \underline{A}$.
- It is a subset $\mathrm{Pol}_n(\underline{A}) \subseteq A^{A^n}$.
- It is pp-definable.
- It has an action of $S_n = \mathrm{Sym}(n)$ by permuting entries.
- The action is pp-definable.

Part 3

If $\underline{A}$ has not fully symmetric polymorphism of an arity n, then $\underline{A}$ pp-constructs $S(G \curvearrowright \mathbb{P}(G))$ for G finite simple group.

- Consider all polymorphisms $\underline{A}^n \to \underline{A}$.
- It is a subset $\mathrm{Pol}_n(\underline{A}) \subseteq A^{A^n}$.
- It is pp-definable.
- It has an action of $S_n = \mathrm{Sym}(n)$ by permuting entries.
- The action is pp-definable.
- The action $S_n \curvearrowright \mathrm{Pol}_n(\underline{A})$ has no fixed point.

Part 3

If $\underline{A}$ has not fully symmetric polymorphism of an arity n, then $\underline{A}$ pp-constructs $S(G \curvearrowright \mathbb{P}(G))$ for G finite simple group.

- Consider all polymorphisms $\underline{A}^n \to \underline{A}$.
- It is a subset $\mathrm{Pol}_n(\underline{A}) \subseteq A^{A^n}$.
- It is pp-definable.
- It has an action of $S_n = \mathrm{Sym}(n)$ by permuting entries.
- The action is pp-definable.
- The action $S_n \curvearrowright \mathrm{Pol}_n(\underline{A})$ has no fixed point.

$\underline{A}$ pp-constructs a group action without fixed point, namely $S(S_n \curvearrowright \mathrm{Pol}_n(\underline{A}))$.

Part 3

What is the simplest group we can get from $S(G \curvearrowright X)$?

Part 3

What is the simplest group we can get from $S(G \curvearrowright X)$?

1. If $H \leq G$, $H \curvearrowright X$ without fixed point, then $S(G \curvearrowright X)$ pp-constructs $S(H \curvearrowright X)$.

Part 3

What is the simplest group we can get from $S(G \curvearrowright X)$?

1. If $H \leq G$, $H \curvearrowright X$ without fixed point, then $S(G \curvearrowright X)$ pp-constructs $S(H \curvearrowright X)$.
2. If $N \trianglelefteq G$, $N \curvearrowright X$ trivial, then $S(G \curvearrowright X)$ pp-constructs $S(G/N \curvearrowright X)$.

Part 3

What is the simplest group we can get from $S(G \curvearrowright X)$?

1. If $H \leq G$, $H \curvearrowright X$ without fixed point, then $S(G \curvearrowright X)$ pp-constructs $S(H \curvearrowright X)$.
2. If $N \trianglelefteq G$, $N \curvearrowright X$ trivial, then $S(G \curvearrowright X)$ pp-constructs $S(G/N \curvearrowright X)$.
3. If $N \trianglelefteq G$, $N \curvearrowright X$ with fixed points, then

   $$\mathrm{Fix}(N) = \{x \in X \mid N.x = x\}$$

   is closed under G action. Moreover, $S(G \curvearrowright X)$ pp-constructs $S(G \curvearrowright \mathrm{Fix}(N))$ and $S(G/N \curvearrowright \mathrm{Fix}(N))$.

Part 3

What is the simplest group we can get from $S(G \curvearrowright X)$?

1. If $H \leq G$, $H \curvearrowright X$ without fixed point, then $S(G \curvearrowright X)$ pp-constructs $S(H \curvearrowright X)$.
2. If $N \trianglelefteq G$, $N \curvearrowright X$ trivial, then $S(G \curvearrowright X)$ pp-constructs $S(G/N \curvearrowright X)$.
3. If $N \trianglelefteq G$, $N \curvearrowright X$ with fixed points, then

$$\mathrm{Fix}(N) = \{x \in X \mid N.x = x\}$$

is closed under G action. Moreover, $S(G \curvearrowright X)$ pp-constructs $S(G \curvearrowright \mathrm{Fix}(N))$ and $S(G/N \curvearrowright \mathrm{Fix}(N))$.

What is left?

G simple, every maximal subgroup of G has a fixed point

Part 4

$S(G \curvearrowright \mathbb{P}(G))$ does not pp-construct $S(G' \curvearrowright \mathbb{P}(G'))$ for $G \neq G'$ different, finite simple.

Definition

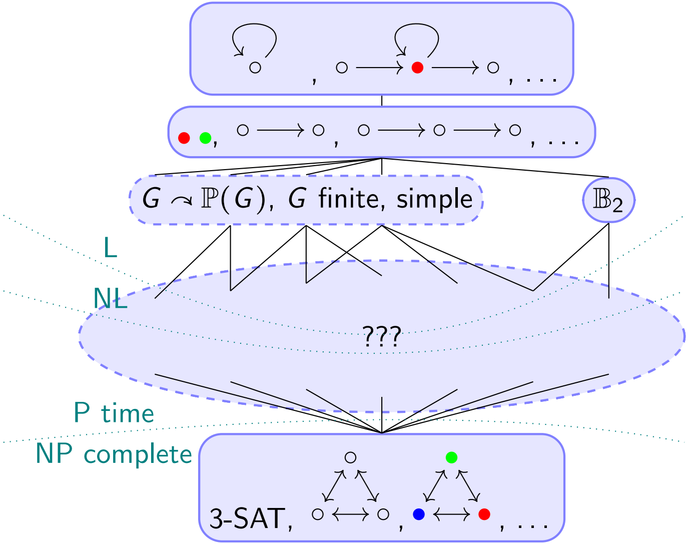
For $G \curvearrowright X$, define the minor condition $\Sigma(G \curvearrowright X)$ as $\exists f \in \mathrm{Pol}_{|X|}(\underline{A})$,

$$\forall g \in G : f(x_1, \ldots, x_{|X|}) = f(x_{g.1}, \ldots, x_{g.|X|})$$

- $S(G \curvearrowright X)$ does not satisfy $\Sigma(G \curvearrowright X)$.
- If $S(G \curvearrowright X)$ does not satisfy $\Sigma(H \curvearrowright Y)$, then
  - there is no appropriate map $X^Y \to X$,
  - there is a problem child m in $X^Y = \mathrm{map}(Y, X)$,
  - there are subgroups $G'_m \trianglelefteq G_m \leq G$, $H'_m \trianglelefteq H_m \leq H$ such that $G_m \curvearrowright X, H_m \curvearrowright Y$ nontrivial and $G_m/G'_m \cong H_m/H'_m \ncong \{1\}$.

$S(G \curvearrowright \mathbb{P}(G))$ satisfies $\Sigma(G' \curvearrowright \mathbb{P}(G'))$ but not $\Sigma(G \curvearrowright \mathbb{P}(G))$ □

The PP-Constructability Poset on Finite Structures



Thank you for your attention

Funding statement: Funded by the European Union (ERC, POCOCOP, 101071674).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.