# Proof complexity of Mal'tsev CSP

Azza Gaysin

Weak Arithmetics Days 44

09.09.2025

# Constraint Satisfaction problems

**Definition 1 (Constraint Satisfaction problems).**

The problem CSP($\Gamma$) consists of a finite set $A$ and a finite collection $\Gamma = \{R_1, ..., R_n\}$ of relations on $A$ - constraint language. The question is, given as input a list of variables $V$ and a list of constraints $\mathcal{C} = \{C_1, ..., C_m\}$, where $C_i = (\bar{x}_i, R_i)$, whether there is an assignment of variables to values in $A$ satisfying the given constraints.

- For a fixed $n$, the problem $n$-coloring, $A = \{0, 1, ..., n-1\}$, $\Gamma$ contains the only binary relation $\neq_n := \{(a, b) : a \neq b\}$;
- The problem of $\mathcal{H}$-coloring, a homomorphism problem between two graphs, $A = V_{\mathcal{H}}$ and $\Gamma$ contains the only binary relation $E_{\mathcal{H}}$. If $\mathcal{H}$ is a complete undirected graph $\mathcal{K}_n$, then the problem $\mathcal{K}_n$-coloring reduces to $n$-coloring.

# Constraint Satisfaction problems

**Definition 1 (Constraint Satisfaction problems).**

The problem CSP($\Gamma$) consists of a finite set $A$ and a finite collection $\Gamma = \{R_1, ..., R_n\}$ of relations on $A$ - constraint language. The question is, given as input a list of variables $V$ and a list of constraints $\mathcal{C} = \{C_1, ..., C_m\}$, where $C_i = (\bar{x}_i, R_i)$, whether there is an assignment of variables to values in $A$ satisfying the given constraints.

- For a fixed $n$, the problem $n$-coloring, $A = \{0, 1, ..., n-1\}$, $\Gamma$ contains the only binary relation $\neq_n := \{(a, b) : a \neq b\}$;
- The problem of $\mathcal{H}$-coloring, a homomorphism problem between two graphs, $A = V_{\mathcal{H}}$ and $\Gamma$ contains the only binary relation $E_{\mathcal{H}}$. If $\mathcal{H}$ is a complete undirected graph $\mathcal{K}_n$, then the problem $\mathcal{K}_n$-coloring reduces to $n$-coloring.

**Definition 2 (CSP as a Homomorphism problem).**

Let $\mathcal{A}$ be a fixed relational structure over vocabulary $R_1$,..., $R_n$. An *instance of the constraint satisfaction problem* CSP($\mathcal{A}$) is any relational structure $\mathcal{X}$ over the same vocabulary. The question is whether there exists a homomorphism from $\mathcal{X}$ to $\mathcal{A}$. $\mathcal{A}$ is called a target structure and $\mathcal{X}$ an instance structure.

# Complexity of CSP

**Theorem 3 (CSP dichotomy theorem, Zhuk, Bulatov 2017).**

*For each finite constraint language $\Gamma$ over finite domain $A$, CSP ($\Gamma$) is either polynomial time or NP-complete.*

# Complexity of CSP

**Theorem 3 (CSP dichotomy theorem, Zhuk, Bulatov 2017).**

*For each finite constraint language $\Gamma$ over finite domain $A$, CSP ($\Gamma$) is either polynomial time or NP-complete.*

**Definition 4 (Polymorphism).**

We say that an $m$-ary operation $f : A^m \to A$ *preservers* an $n$-ary relation $R \in A^n$ (or $f$ is a *polymorphism* of $R$, or $R$ is *invariant* under $f$) if $f(\bar{a_1}, ..., \bar{a_m}) \in R$ for all choices of $\bar{a_1}, ..., \bar{a_m} \in R$.

$$\begin{bmatrix} a_{11} \\ a_{21} \\ ... \\ a_{m1} \end{bmatrix} \in R, ...., \begin{bmatrix} a_{1n} \\ a_{2n} \\ ... \\ a_{mn} \end{bmatrix} \in R \implies \begin{bmatrix} f(a_{11}, & ..., & a_{1n}) \\ f(a_{21}, & ..., & a_{2n}) \\ ... & ..., & ... \\ f(a_{m1}, & ..., & a_{mn}) \end{bmatrix} \in R$$

# Complexity of CSP

**Theorem 3 (CSP dichotomy theorem, Zhuk, Bulatov 2017).**

*For each finite constraint language $\Gamma$ over finite domain $A$, CSP ($\Gamma$) is either*

*polynomial time or NP-complete.*

**Definition 4 (Polymorphism).**

We say that an $m$-ary operation $f : A^m \to A$ *preservers* an $n$-ary relation $R \in A^n$ (or $f$ is a *polymorphism* of $R$, or $R$ is *invariant* under $f$) if $f(\bar{a_1}, ..., \bar{a_m}) \in R$ for all choices of $\bar{a_1}, ..., \bar{a_m} \in R$.

$$\begin{bmatrix} a_{11} \\ a_{21} \\ ... \\ a_{m1} \end{bmatrix} \in R, ...., \begin{bmatrix} a_{1n} \\ a_{2n} \\ ... \\ a_{mn} \end{bmatrix} \in R \implies \begin{bmatrix} f(a_{11}, & ..., & a_{1n}) \\ f(a_{21}, & ..., & a_{2n}) \\ ... & ..., & ... \\ f(a_{m1}, & ..., & a_{mn}) \end{bmatrix} \in R$$

**Theorem 5.**

*For any relational structure $\mathcal{A} = (A, \Gamma)$, there exists an algebra $\mathbb{A} = (A, F)$ such that*

$$Clone(F) = Pol(\Gamma).$$

# Mal'tsev CSP

**Definition 6 (Mal'tsev term).**

A ternary operation $\mu : A^3 \to A$ on a finite set $A$ is called *Mal'tsev* if it satisfies the identities $\mu(x, y, y) = \mu(y, y, x) = x$. An algebra with a Mal'tsev term is called a *Mal'tsev algebra*.

- For a field $F$, Mal'tsev operation is given by $\mu(x, y, z) = x - y + z$.
- For a multiplicative group $G$, Mal'tsev operation is given by $\mu(x, y, z) = xy^{-1}z$.

# Mal'tsev CSP

**Definition 6 (Mal'tsev term).**

A ternary operation $\mu : A^3 \to A$ on a finite set $A$ is called *Mal'tsev* if it satisfies the identities $\mu(x, y, y) = \mu(y, y, x) = x$. An algebra with a Mal'tsev term is called a *Mal'tsev algebra*.

- For a field $F$, Mal'tsev operation is given by $\mu(x, y, z) = x - y + z$.
- For a multiplicative group $G$, Mal'tsev operation is given by $\mu(x, y, z) = xy^{-1}z$.

**Example 7 (Mal'tsev CSP).**

An instance of the *3-LIN(p) problem* is a system of linear equations $A \cdot \boldsymbol{x} = \boldsymbol{b}$ over the field $\mathbb{Z}_p$, where each equation involves three variables. If $R$ is the solution space of $A \cdot \boldsymbol{x} = \boldsymbol{b}$, then $\mu(x, y, z) = x - y + z$ is a polymorphism of $R$: suppose that $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in R$, then $\mu(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in R$ since

$$A \cdot \mu(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = A \cdot (\boldsymbol{x} - \boldsymbol{y} + \boldsymbol{z}) = A \cdot \boldsymbol{x} - A \cdot \boldsymbol{y} + A \cdot \boldsymbol{z} = \boldsymbol{b} - \boldsymbol{b} + \boldsymbol{b} = \boldsymbol{b}.$$

# Mal'tsev CSP

**Definition 6 (Mal'tsev term).**

A ternary operation $\mu : A^3 \to A$ on a finite set $A$ is called *Mal'tsev* if it satisfies the identities $\mu(x, y, y) = \mu(y, y, x) = x$. An algebra with a Mal'tsev term is called a *Mal'tsev algebra*.

- For a field $F$, Mal'tsev operation is given by $\mu(x, y, z) = x - y + z$.
- For a multiplicative group $G$, Mal'tsev operation is given by $\mu(x, y, z) = xy^{-1}z$.

**Example 7 (Mal'tsev CSP).**

An instance of the *3-LIN(p) problem* is a system of linear equations $A \cdot \boldsymbol{x} = \boldsymbol{b}$ over the field $\mathbb{Z}_p$, where each equation involves three variables. If $R$ is the solution space of $A \cdot \boldsymbol{x} = \boldsymbol{b}$, then $\mu(x, y, z) = x - y + z$ is a polymorphism of $R$: suppose that $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in R$, then $\mu(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in R$ since

$$A \cdot \mu(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = A \cdot (\boldsymbol{x} - \boldsymbol{y} + \boldsymbol{z}) = A \cdot \boldsymbol{x} - A \cdot \boldsymbol{y} + A \cdot \boldsymbol{z} = \boldsymbol{b} - \boldsymbol{b} + \boldsymbol{b} = \boldsymbol{b}.$$

**Theorem 8 (Bulatov, Dalmau 2006).**

*Let $\mu$ be a Mal'tsev operation. Then CSP($Inv(\mu)$), where $Inv(\mu)$ is the set of all relations on $A$ invariant under $\mu$, is solvable in polynomial time.*

# Compact representations

**Definition 9 (Signature).**

- For any tuple $(i, a, b)$ with $i \in [n]$, $a, b \in A$, a *realization* of $(i, a, b)$ is any pair $t_a, t_b \in A^n$ such that

$$\pi_{1,\ldots,i-1}(t_a) = \pi_{1,\ldots,i-1}(t_b) \quad \text{and} \quad \pi_i(t_a) = a, \pi_i(t_b) = b.$$

  The pair $t_a, t_b$ *witnesses* the tuple $(i, a, b)$.

- The *signature* $Sig(R)$ of $R \subseteq A^n$ is the set of all tuples $(i, a, b)$ witnessed by tuples in $R$, i.e.:

$$Sig(R) = \{(i, a, b) \in [n] \times A^2 : \exists t_a, t_b \in R \text{ s.t. } (t_a, t_b) \text{ witnesses } (i, a, b)\}.$$

# Compact representations

**Definition 9 (Signature).**

- For any tuple $(i, a, b)$ with $i \in [n]$, $a, b \in A$, a *realization* of $(i, a, b)$ is any pair $t_a, t_b \in A^n$ such that

$$\pi_{1,\ldots,i-1}(t_a) = \pi_{1,\ldots,i-1}(t_b) \quad \text{and} \quad \pi_i(t_a) = a, \pi_i(t_b) = b.$$

  The pair $t_a, t_b$ *witnesses* the tuple $(i, a, b)$.
- The *signature* $Sig(R)$ of $R \subseteq A^n$ is the set of all tuples $(i, a, b)$ witnessed by tuples in $R$, i.e.:

$$Sig(R) = \{(i, a, b) \in [n] \times A^2 : \exists t_a, t_b \in R \text{ s.t. } (t_a, t_b) \text{ witnesses } (i, a, b)\}.$$

**Definition 10 (Representation).**

A subset $R' \subseteq R$ is called a *representation* of $R$ if $Sig(R) = Sig(R')$, and if $|R'| \leq 2|Sig(R)|$ we call it *compact*.

- Every relation $R$ has a compact representation: for every element $(i, a, b) \in Sig(R)$ it is enough to take only two elements $t_a, t_b$ that witness the tuple.
- If $R'$ is a minimal representation of $R \subseteq A^n$, then $|R'| \leq 2n \cdot |A|^2$.

# Compact representations

**Example 11.**

Consider $\mathbb{A}^n$, and fix some $d \in A$. For any $i \in [n]$ and any $a \in A$ we define an element $e_{i,a}$ as the only element satisfying:

$$e_{i,a} := \begin{cases} a \text{ if } i = j, \\ d \text{ otherwise.} \end{cases}$$

For every tuple $(i, a, b)$ a pair $(e_{i,a}, e_{i,b})$ witnesses the tuple, and the set of elements $\{e_{i,a} : i \in [n], a \in A\}$ is a compact representation of a relation $A^n$.

# Compact representations

**Example 11.**

Consider $\mathbb{A}^n$, and fix some $d \in A$. For any $i \in [n]$ and any $a \in A$ we define an element $e_{i,a}$ as the only element satisfying:

$$e_{i,a} := \begin{cases} a \text{ if } i = j, \\ d \text{ otherwise.} \end{cases}$$

For every tuple $(i, a, b)$ a pair $(e_{i,a}, e_{i,b})$ witnesses the tuple, and the set of elements $\{e_{i,a} : i \in [n], a \in A\}$ is a compact representation of a relation $A^n$.

**Theorem 12.**

*Suppose that $\mathbb{A}$ has a Mal'tsev term $\mu$ and $\mathbb{R} \leq \mathbb{A}^n$. Let $R' \subseteq \mathbb{R}$ be a subset with $Sig(R') = Sig(\mathbb{R})$. Then $\mathbb{R}$ is generated by $R'$ using only $\mu$.*

- Let $\mathbb{R}' \leq \mathbb{R}$ be generated by $R'$ using $\mu$. Then by induction on $i$ we prove that

$$\pi_{1,\ldots,i}(\mathbb{R}') = \pi_{1,\ldots,i}(\mathbb{R}).$$

# Mal'tsev Algorithm

**The idea of Mal'tsev algorithm:**

1. Consider any CSP instance $\mathcal{P} = (\{x_1, ..., x_n\}, A, \{C_1, ..., C_m\})$, where every relation from $C_1, ..., C_m$ is invariant under a Mal'tsev term $\mu$.
2. For each $l \in \{0, ..., m\}$ define an instance $\mathcal{P}_l = (\{x_1, ..., x_n\}, A, \{C_1, ..., C_l\})$ as the CSP instance that contains the first $l$ constraints of $\mathcal{P}$. Denote by $\mathbb{R}_l$ the $n$-ary relation on $A$ defined as:

$$\mathbb{R}_l = \{(s(x_1), ..., s(x_n)) : s \text{ is a solution of } \mathcal{P}_l\}.$$

# Mal'tsev Algorithm

**The idea of Mal'tsev algorithm:**

1. Consider any CSP instance $\mathcal{P} = (\{x_1, ..., x_n\}, A, \{C_1, ..., C_m\})$, where every relation from $C_1, ..., C_m$ is invariant under a Mal'tsev term $\mu$.
2. For each $l \in \{0, ..., m\}$ define an instance $\mathcal{P}_l = (\{x_1, ..., x_n\}, A, \{C_1, ..., C_l\})$ as the CSP instance that contains the first $l$ constraints of $\mathcal{P}$. Denote by $\mathbb{R}_l$ the $n$-ary relation on $A$ defined as:

$$\mathbb{R}_l = \{(s(x_1), ..., s(x_n)) : s \text{ is a solution of } \mathcal{P}_l\}.$$

3. Compute for each $l \in \{0, ..., m\}$ a compact representation $R_l$ of $\mathbb{R}_l$.
   - In the initial case for $l = 0$, $\mathcal{P}_0$ has no constraints at all, so $\mathbb{R}_0 = \mathbb{A}^n$. The compact representation is the set $\{e_{i,a} : i \in [n], a \in A\}$.
   - Start an iterative process in which a compact representation $R_l$ of $\mathbb{R}_l$ is obtained from $R_{l-1}$ and the constraint $C_l$ with the use of some procedure Next$(R_{l-1}, C_l)$.

# Proof complexity

**A homomorphism problem between relational structures $\mathcal{X} \to \mathcal{A}$:**

- For every element $i$ in $\mathcal{X}$ and element $j$ in $\mathcal{A}$ set propositional atom $p_{ij}$;
- For every map $h$ from $\mathcal{X}$ to $\mathcal{A}$ set $p_{ij}$ to truth if and only if $h(i) = j$.

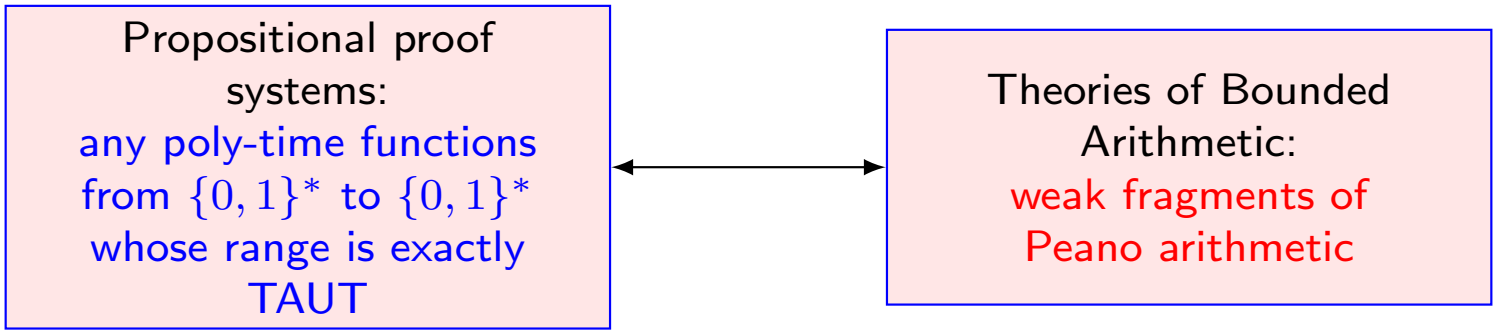
**For unsatisfiable instances $\mathcal{X} \to \mathcal{A}$ the formula $\neg\,\mathrm{pHom}(\mathcal{X}, \mathcal{A})$ is a tautology.**

# Proof complexity

**A homomorphism problem between relational structures $\mathcal{X} \to \mathcal{A}$:**

- For every element $i$ in $\mathcal{X}$ and element $j$ in $\mathcal{A}$ set propositional atom $p_{ij}$;
- For every map $h$ from $\mathcal{X}$ to $\mathcal{A}$ set $p_{ij}$ to truth if and only if $h(i) = j$.

**For unsatisfiable instances $\mathcal{X} \to \mathcal{A}$ the formula $\neg\,\mathrm{pHom}(\mathcal{X}, \mathcal{A})$ is a tautology.**




- A proof system can be viewed as a nonuniform counterpart of the universal fragment of a theory: the universal statements provable within the theory translate into families of tautologies with short proofs in the corresponding proof system.

# The Goal

**The goal** is to establish an upper bound of the proof complexity of CSPs with a Mal'tsev term, in the sense that a propositional formula expressing that an instance of CSP is unsatisfiable has a short proof in a proof system $P$.

- For this, we first prove the universal statement of unsatisfiability in the B.A. theory $T$ corresponding to $P$, and then apply a translation theorem.

# The Goal

**The goal** is to establish an upper bound of the proof complexity of CSPs with a Mal'tsev term, in the sense that a propositional formula expressing that an instance of CSP is unsatisfiable has a short proof in a proof system $P$.

- For this, we first prove the universal statement of unsatisfiability in the B.A. theory $T$ corresponding to $P$, and then apply a translation theorem.
- To prove the universal statement, it is enough to prove the soundness of Mal'tsev algorithm. Assume that the theory $T$ proves: for every $0 < l < m$, if $R_{l-1}$ is a compact representation of $\mathbb{R}_{l-1}$, then $\mathsf{Next}(R_{l-1}, C_l)$ outputs a compact representation of $\mathbb{R}_l$. Then the formula

$$R_0 = \{e_{i,a} : (i,a) \in [n] \times D_i\} \wedge R_m = \emptyset \wedge$$
$$\wedge \forall 0 < l \leq m \; R_l := \mathsf{Next}(R_{l-1}, C_l)$$

  will be a proof of unsatisfiability.

# Formalization: Set-Up

- **Second-sorted theories:**
  - variables $x, y, z, \ldots$ of the first kind are called *number variables*, and $X, Y, Z, \ldots$ of the second kind are called *set variables*;
  - Sets code universes, functions and relations using one-to-one pairing function $\langle x, y \rangle$.
  - $\Sigma_0^{1,b}$-formulas contain bounded quantification over number variables $\forall x < t, \exists x < t$;
  - $\Sigma_1^{1,b}$-formulas also contain bounded existential quantification over set variables $\exists X\, |X| < t$.

# Formalization: Set-Up

- **Second-sorted theories:**
  - variables $x, y, z, \ldots$ of the first kind are called *number variables*, and $X, Y, Z, \ldots$ of the second kind are called *set variables*;
  - Sets code universes, functions and relations using one-to-one pairing function $\langle x, y \rangle$.
  - $\Sigma_0^{1,b}$-formulas contain bounded quantification over number variables $\forall x < t, \exists x < t$;
  - $\Sigma_1^{1,b}$-formulas also contain bounded existential quantification over set variables $\exists X\, |X| < t$.

**Definition 13 (Theory $V^1$).**

A bounded arithmetic *theory* $V^1$ is

1. a two-sorted theory, the language $\mathcal{L}^2{}_{\mathcal{PA}} = \{0, 1, +, \cdot, |\,|, =_1, =_2, \leq, \in\}$;
2. accepts the IND scheme for all $\Sigma_1^{1,b}$-formulas $\varphi$:

$$\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(x+1)) \to \forall z \varphi(z)$$

3. accepts bounded comprehension axiom $\Sigma_0^{1,b}$-CA:

$$\forall x \exists X\ |X| \leq x\, \forall y < x\ \ y \in X \iff \varphi(y).$$

- $V^1$ corresponds to polynomial time reasoning (the functions definable in $V^1$ are those computable in FP).

# Formalization: Set-Up

**Definition 14 (Extended Frege proof system).**

A propositional *Frege proof system* $F$ is a finite set of Frege rules that is sound and implicationally complete, meaning that for any propositional formulas $\varphi_1, ..., \varphi_n, \psi$,

$$\varphi_1, ..., \varphi_n \vDash \psi \iff \varphi_1, ..., \varphi_n \vdash_F \psi.$$

In *extended Frege proof system* we are additionally allowed to abbreviate formulas with propositional variables.

- A well-known example of a Frege rule is a modus ponens:

$$\frac{\varphi \quad \varphi \to \psi}{\psi}$$

**Theorem 1 ($V^1$ Translation).**

*Suppose that $\varphi(\bar{x}, \bar{X})$ is a $\Sigma_0^{1,b}$-formula such that $V^1 \vdash \forall \bar{x} \forall \bar{X} \varphi(\bar{x}, \bar{X})$. Then the family of propositional formulas $||\varphi(\vec{x}, \vec{X})|| = \{\varphi(\vec{x}, \vec{X})[\vec{m}, \vec{n}] : \vec{m}, \vec{n} \in \mathbb{N}\}$ has polynomial size extended Frege proofs and these proofs can be constructed by a $p$-time algorithm.*

# Formalization: Set-Up

- We consider constraint languages with at most binary relations (does not affect the result);
- We consider a binary CSP problem as a homomorphism problem between a *directed input graph* encoded as a pair $\mathcal{X} = ([n], E_{\mathcal{X}})$ with $E_{\mathcal{X}}(i, j)$ being a binary relation on $[n]$, and a *directed target graph with domains* encoded as a tuple of sets $\ddot{\mathcal{A}} = ([q], V_{\ddot{\mathcal{A}}}, E_{\ddot{\mathcal{A}}})$, where
  - $V_{\ddot{\mathcal{A}}} < \langle n, q \rangle$ is the set corresponding to the superdomain, and $V_{\ddot{\mathcal{A}}}(i, a)$ indicates that a domain for variable $x_i$ contains element $a$. We denote sets $V_{\ddot{\mathcal{A}}}^{[i]}$ by $D_i$.
  - $E_{\ddot{\mathcal{A}}} < \langle n, n, q, q \rangle$ is the set encoding that there is an edge $(a, b)$ between $D_i$ and $D_j$ if:
$$E_{\ddot{\mathcal{A}}}^{[ij]}(a, b) \to D_i(a) \wedge D_j(b). \tag{1}$$
- An instance of CSP($\mathcal{A}$) is a pair of sets $\Theta = (\mathcal{X}, \ddot{\mathcal{A}})$, satisfying all above conditions.
- A *homomorphism* from $\mathcal{X}$ to $\ddot{\mathcal{A}}$ is a set $H \leq \langle n, q \rangle$ sending each $i \in [n]$ to domain $D_i$ in $V_{\ddot{\mathcal{A}}}$, which can be expressed by $\Sigma_0^{1,b}$-formula $\mathrm{Hom}(\mathcal{X}, \ddot{\mathcal{A}}, H)$.

# Formalization: Set-Up

- A fixed algebra $\mathbb{A}$ of size $q$ with a Mal'tsev term $\mu$ is presented as a pair os sets $\mathbb{A} = ([q], M)$, where $M(a_1, a_2, a_3) = b$;
- We encode a compact representation $R$ as a set $R(i, a, b, j, c)$, where the first three indices represent a tuple $(i, a, b)$ witnessed by a map $T_a$ from $[n]$ to $[D_1, ..., D_n]$, and the last indices define a map itself;
- We consider the sequence of CSP instances $\mathcal{X}_0 := ([n], E_{\mathcal{X}_0})$, ..., $\mathcal{X}_m := ([n], E_{\mathcal{X}_m})$ where $\mathcal{X}_m = \mathcal{X}$, $E_{\mathcal{X}_0}$ is an empty set, and every $\mathcal{X}_{i-1}$ is constructed from the instance $\mathcal{X}_i$ by removing one edge.
- We collect compact representations $R_0, ..., R_m$ of $\mathscr{R}_{\Theta_0}, ..., \mathscr{R}_{\Theta_m}$ to one set $R$ such that for all $a < q, i < n$, and $d_j = min(D_j)$

$$R_{[0]}(i, a, b, , i, a) \wedge \forall j \neq i < n \, R_{[0]}(i, a, b, j, d_j),$$

$$\forall 0 < l \leq m \; R_{[l]} = next(R_{[l-1]}, min(E_{\mathcal{X}_l}), E_{\ddot{\mathcal{A}}}^{min(E_{\mathcal{X}_l})}).$$

# Results

- We define all the sets used in the formalization of Mal'tsev algorithm with $\Sigma_0^{1,b}$-formulas;
- We construct all the sets used in the formalization of Mal'tsev algorithm with $\Sigma_1^{1,b}$-induction;
- $V^1$ proves the correctness of all subroutines of the function $next$;

# Results

- We define all the sets used in the formalization of Mal'tsev algorithm with $\Sigma_0^{1,b}$-formulas;
- We construct all the sets used in the formalization of Mal'tsev algorithm with $\Sigma_1^{1,b}$-induction;
- $V^1$ proves the correctness of all subroutines of the function $next$;

**Theorem 15.**

*For any relational structure $\mathcal{A}$ that corresponds to an algebra with Mal'tsev operation, the theory $V^1$ proves the soundness of Mal'tsev algorithm:*

$$V^1 \vdash \forall \mathcal{X} \forall \ddot{A} \forall R \forall T \ \ (Comp(R, \mathcal{X}, \ddot{A}) \wedge R^{[m]} = \emptyset \longrightarrow \neg Hom(\mathcal{X}, \ddot{A}, T)).$$

**Theorem 16 (Mal'tsev Upper Bound).**

*For any relational structure $\mathcal{A}$ that corresponds to an algebra with Mal'tsev operation, there exists a $p$-time algorithm such that for any unsatisfiable instance $\mathcal{X}$ the output of the algorithm on $\mathcal{X}$ is a propositional proof of the proposition translation of formula $\neg\mathrm{Hom}(\mathcal{X}, \mathcal{A})$ in extended Frege proof system.*

# Corresponding results

**Definition 17 (Generalized majority-minority term).**

Let $k \geq 3$. A $k$-ary operation for $\varphi : A^k \to A$ on a finite set $A$ is called *generalized majority-minority* if for all $a, b \in A$,

$$\varphi(x, y, ..., y) = \varphi(y, x, ..., y) = .... = \varphi(y, y, ..., x) = y \text{ for all } x, y \in \{a, b\}$$

or

$$\varphi(x, y, ..., y) = \varphi(y, y, ..., x) = x \text{ for all } x, y \in \{a, b\}.$$

**Theorem 18 (Dalmau 2005).**

*Let $\varphi$ be a GMM operation. Then CSP($Inv(\varphi)$), where $Inv(\varphi)$ is the set of all relations on $A$ invariant under $\varphi$, is solvable in polynomial time.*

# Corresponding results

**Theorem 19.**

*For any relational structure $\mathcal{A}$ that corresponds to an algebra with GMM operation, the theory $V^1$ proves the soundness of Dalmau's algorithm:*

$$V^1 \vdash \forall\mathcal{X}\forall\ddot{\mathcal{A}}\forall R\forall T\ \ (Comp(R,\mathcal{X},\ddot{\mathcal{A}}) \wedge R^{[m]} = \emptyset \longrightarrow \neg Hom(\mathcal{X},\ddot{\mathcal{A}},T)).$$

**Theorem 20 (GMM Upper Bound).**

*For any relational structure $\mathcal{A}$ that corresponds to an algebra with GMM operation, there exists a $p$-time algorithm such that for any unsatisfiable instance $\mathcal{X}$ the output of the algorithm on $\mathcal{X}$ is a propositional proof of the proposition translation of formula $\neg\mathrm{Hom}(\mathcal{X},\mathcal{A})$ in extended Frege proof system.*

- **Future work:** an algebra $\mathbb{A}$ is said to have *few subpowers* if every subalgebra of $\mathbb{A}^n$ has a (nice) generating set of size $O(n^k)$ for some fixed $k$. The Few Subpowers algorithm was heavily influenced by Dalmau's GMM algorithm.

Thank you!