Short definitions in constraint languages

Jakub Bulín, **Michael Kompatscher**

Charles University

28.08.2023

MFCS - Bordeaux

Short pp-definitions

Structures with short pp-definitions

$\mathbb{A} = (A; R_1, \dots, R_k)$... finite relational structure
$Q \subseteq A^n$ is **pp-definable** over $\mathbb{A}$ if

$$Q(x_1, \dots, x_n) \Leftrightarrow \underbrace{\exists y_1, \dots, y_k \, R_{i_1}(\dots) \wedge \dots \wedge R_{i_j}(\dots)}_{\psi(x_1,\dots,x_n) \text{ pp-formula over } \mathbb{A}}$$

$\langle \mathbb{A} \rangle :=$ all pp-definable relations

Definition

- $\mathbb{A}$ has **pp-definitions of length** $\leq f(n)$ if $\forall Q \in \langle \mathbb{A} \rangle \cap A^n$:
  Q is definable by a pp-formula ψ with $|\psi| \leq f(n)$
- $\mathbb{A}$ has **short pp-definitions** if $\mathbb{A}$ has pp-definitions of length $\leq p(n)$, for a *polynomial* $p(n)$.

Question: Which $\mathbb{A}$ have short pp-definitions?

Examples

Affine spaces

$\mathbb{A} = (\{0,1\}; \{(x,y,z) \mid x + y = z\}, \{0\}, \{1\})$,
$Q \in \langle \mathbb{A} \rangle \Leftrightarrow Q$ affine subspace of $\mathbb{Z}_2^n$
$\Leftrightarrow$ given by $\leq n$ equations:

$$x_{i_1} + x_{i_2} + \ldots + x_{i_k} = a \Leftrightarrow$$
$$\exists y_2, \ldots, y_k : (x_{i_1} + x_{i_2} = y_2) \wedge (y_2 + x_{i_3} = y_3) \wedge \ldots \wedge (y_{k-1} + x_k = y_k) \wedge (y_k = a).$$

$\Rightarrow$ pp-definitions of length $O(n^2)$.

Examples

Affine spaces

$\mathbb{A} = (\{0,1\}; \{(x,y,z) \mid x+y=z\}, \{0\}, \{1\})$,
$Q \in \langle \mathbb{A} \rangle \Leftrightarrow Q$ affine subspace of $\mathbb{Z}_2^n$
$\Leftrightarrow$ given by $\leq n$ equations:

$$x_{i_1} + x_{i_2} + \ldots + x_{i_k} = a \Leftrightarrow$$
$$\exists y_2, \ldots, y_k : (x_{i_1} + x_{i_2} = y_2) \wedge (y_2 + x_{i_3} = y_3) \wedge \ldots \wedge (y_{k-1} + x_k = y_k) \wedge (y_k = a).$$

$\Rightarrow$ pp-definitions of length $O(n^2)$.

2-SAT

$\mathbb{A} = (\{0,1\}; (R_{a,b})_{a,b \in \{0,1\}})$, with $R_{a,b} = \{0,1\}^2 \setminus \{(a,b)\}$.

$$Q \in \langle \mathbb{A} \rangle \Leftrightarrow Q(x_1, \ldots, x_n) = \bigwedge_{1 \leq i,j \leq n} \mathrm{pr}_{\{i,j\}} Q(x_i, x_j).$$

$\Rightarrow$ pp-definitions of length $O(n^2)$.

Algebras/Clones with short pp-definitions

Observation 1

$\mathbb{A}$ has pp-defs. of length $\leq p(n)$
$\langle \mathbb{A} \rangle = \langle \mathbb{B} \rangle \Rightarrow \mathbb{B}$ has pp-defs. of length $\leq c \cdot p(n)$

Algebras/Clones with short pp-definitions

Observation 1

$\mathbb{A}$ has pp-defs. of length $\leq p(n)$
$\langle \mathbb{A} \rangle = \langle \mathbb{B} \rangle \Rightarrow \mathbb{B}$ has pp-defs. of length $\leq c \cdot p(n)$

$\mathrm{Pol}(\mathbb{A}) = \{f\colon \mathbb{A}^n \to \mathbb{A} \mid n \in \mathbb{N}\}$... *polymorphism clone of* $\mathbb{A}$
A... algebraic structure
$\mathrm{Inv}(\mathbf{A}) = \{R \leq \mathbf{A}^n \mid n \in \mathbb{N}\}$ *invariant relations of* **A**

$\mathrm{Inv}(\mathrm{Pol}(\mathbb{A})) = \langle \mathbb{A} \rangle \Rightarrow$ short pp-definitions is a **property of** $\mathrm{Pol}(\mathbb{A})$
(even up to clone isomorphism).

Algebras/Clones with short pp-definitions

Observation 1

$\mathbb{A}$ has pp-defs. of length $\leq p(n)$
$\langle\mathbb{A}\rangle = \langle\mathbb{B}\rangle \Rightarrow \mathbb{B}$ has pp-defs. of length $\leq c \cdot p(n)$

$\mathrm{Pol}(\mathbb{A}) = \{f\colon \mathbb{A}^n \to \mathbb{A} \mid n \in \mathbb{N}\}$... *polymorphism clone of* $\mathbb{A}$
A... algebraic structure
$\mathrm{Inv}(\mathbf{A}) = \{R \leq \mathbf{A}^n \mid n \in \mathbb{N}\}$ *invariant relations of* **A**

$\mathrm{Inv}(\mathrm{Pol}(\mathbb{A})) = \langle\mathbb{A}\rangle \Rightarrow$ short pp-definitions is a **property of** $\mathrm{Pol}(\mathbb{A})$
(even up to clone isomorphism).

Definition
A has **short pp-definitions**, if $\mathrm{Inv}(\mathbf{A}) = \langle\mathbb{A}\rangle$ has short pp-definitions.

Examples

- Affine subspaces of $\mathbb{Z}_2^n \leftrightarrow \mathbf{A} = (\{0,1\}, x - y + z)$
- 2-SAT $\leftrightarrow \mathbf{A} = (\{0,1\}, \mathrm{maj}(x,y,z))$

Few subpower algebras

Observation 2

$\mathbb{A}$ has pp-definitions of length $\leq p(n)$
$\Rightarrow |\langle \mathbb{A} \rangle \cap A^n| \leq c^{p(n)}$ for some $c > 1$

Few subpower algebras

Observation 2

$\mathbb{A}$ has pp-definitions of length $\leq p(n)$
$\Rightarrow |\langle \mathbb{A} \rangle \cap A^n| \leq c^{p(n)}$ for some $c > 1$

If p is polynomial, we say $\mathrm{Pol}(\mathbb{A})$ has *few subpowers*.

So **short pp-definitions** $\Rightarrow$ **few subpowers**.

Few subpower algebras

Observation 2

$\mathbb{A}$ has pp-definitions of length $\leq p(n)$
$\Rightarrow |\langle \mathbb{A} \rangle \cap A^n| \leq c^{p(n)}$ for some $c > 1$

If p is polynomial, we say $\mathrm{Pol}(\mathbb{A})$ has *few subpowers*.

So **short pp-definitions** $\Rightarrow$ **few subpowers**.

If $\mathbf{A}$ has few subpowers:

- $\mathbf{A}$ has an edge term t (IMMVW'10):
$$\begin{aligned} t(y, y, x, x, x, \dots, x) &\approx x \\ t(y, x, y, x, x, \dots, x) &\approx x \\ t(x, x, x, y, x, \dots, x) &\approx x \\ &\ddots \\ t(x, x, x, x, x, \dots, y) &\approx x \end{aligned}$$
- $\mathrm{Inv}(\mathbf{A}) = \langle \mathbb{A} \rangle$ for some finite $\mathbb{A} = (A; R_1, \dots, R_n)$ (AMM'14)

A conjecture about few subpowers

Conjecture

Conjecture (Bulín)

- (weak) $\mathbf{A}$ has short pp-defs. $\Leftrightarrow$ $\mathbf{A}$ has few subpowers.
- (strong) $\mathbf{A}$ has pp-defs. of length $O(n^k)$ $\Leftrightarrow$ $\mathbf{A}$ has a k-edge term.

Conjecture

Conjecture (Bulín)

- (weak) **A** has short pp-defs. $\Leftrightarrow$ **A** has few subpowers.
- (strong) **A** has pp-defs. of length $O(n^k)$ $\Leftrightarrow$ **A** has a k-edge term.

True for

- **A** is affine
- **A** has NU-term
  $y \approx t(y, x, \ldots, x) \approx t(x, y, x, \ldots, x) \approx \ldots \approx t(x, \ldots, x, y)$
- $|A| = 2$ (Lagerkvist, Wahlström '14)

Conjecture

Conjecture (Bulín)

- (weak) **A** has short pp-defs. $\Leftrightarrow$ **A** has few subpowers.
- (strong) **A** has pp-defs. of length $O(n^k)$ $\Leftrightarrow$ **A** has a k-edge term.

True for

- **A** is affine
- **A** has NU-term
  $y \approx t(y, x, \ldots, x) \approx t(x, y, x, \ldots, x) \approx \ldots \approx t(x, \ldots, x, y)$
- $|A| = 2$ (Lagerkvist, Wahlström '14)

$|A| = 3$ not covered by above

Main result

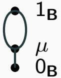
Theorem (Bulín, MK '23)

If $\mathrm{HSP}(\mathbf{A})$ is residually finite, then
$\mathbf{A}$ has pp-definition of length $O(n^k) \Leftrightarrow \mathbf{A}$ has a k-edge term.

Main result

Theorem (Bulín, MK '23)

If HSP($\mathbf{A}$) is residually finite, then
$\mathbf{A}$ has pp-definition of length $O(n^k) \Leftrightarrow \mathbf{A}$ has a k-edge term.

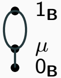
$\mathbf{B}$ is *subdirectly irreducible*, if $\mathrm{Con}(\mathbf{B}) =$ 

HSP($\mathbf{A}$) *residually finite*, if
$\mathbf{B} \in$ HSP($\mathbf{A}$) is SI $\Leftrightarrow \mathbf{B} \in \{\mathbf{B}_1, \ldots, \mathbf{B}_k\}$, $|B_i| < \infty$.

Main result

Theorem (Bulín, MK '23)

If HSP($\mathbf{A}$) is residually finite, then
$\mathbf{A}$ has pp-definition of length $O(n^k) \Leftrightarrow \mathbf{A}$ has a k-edge term.

$\mathbf{B}$ is *subdirectly irreducible*, if $\mathrm{Con}(\mathbf{B}) =$ 

HSP($\mathbf{A}$) *residually finite*, if
$\mathbf{B} \in$ HSP($\mathbf{A}$) is SI $\Leftrightarrow \mathbf{B} \in \{\mathbf{B}_1, \ldots, \mathbf{B}_k\}$, $|B_i| < \infty$.

(folklore) $|A| = 3$, $\mathbf{A}$ few subpowers $\Rightarrow$ HSP($\mathbf{A}$) is residually finite.

Corollary (Bulín, MK '23)

If $|A| = 3$, then
$\mathbf{A}$ has pp-definition of length $O(n^k) \Leftrightarrow \mathbf{A}$ has a k-edge term.

Proof idea

Proof step 1: Reduction to critical relations

A relation $R \leq \mathbf{A}^n$ is called **critical** if

- R is $\wedge$-irreducible ($R_1, R_2 > R \Rightarrow R_1 \cap R_2 > R$)
- R has no dummy variables

Proof step 1: Reduction to critical relations

A relation $R \leq \mathbf{A}^n$ is called **critical** if

- R is $\wedge$-irreducible ($R_1, R_2 > R \Rightarrow R_1 \cap R_2 > R$)
- R has no dummy variables

Lemma

$\mathbf{A}$... k-edge-term, $R \leq \mathbf{A}^n$. Then

$R = \bigwedge_{|J| \leq k} (\mathrm{pr}_J\, R) \wedge R_1 \wedge \ldots \wedge R_l$ for $l \leq n \cdot |A|^2$, R_i critical, *parallelogram property.*

Proof step 1: Reduction to critical relations

A relation $R \leq \mathbf{A}^n$ is called **critical** if

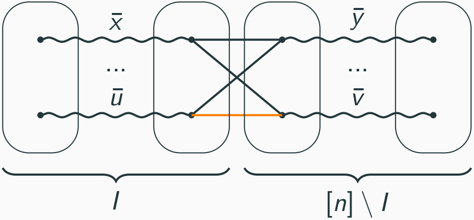
- R is $\wedge$-irreducible ($R_1, R_2 > R \Rightarrow R_1 \cap R_2 > R$)
- R has no dummy variables

Lemma

$\mathbf{A}$... k-edge-term, $R \leq \mathbf{A}^n$. Then

$R = \bigwedge_{|J| \leq k} (\mathrm{pr}_J\, R) \wedge R_1 \wedge \ldots \wedge R_l$ for $l \leq n \cdot |A|^2$, R_i critical, *parallelogram property.*

$R \subseteq A^n$ has the **parallelogram property** if $\forall I \subset [n]$



$(\bar{x}, \bar{y}), (\bar{x}, \bar{v}), (\bar{u}, \bar{y}) \in R$

$\Rightarrow (\bar{u}, \bar{v}) \in R$

Proof step 2: Similarity

Task: find short pp-definitions for $R \leq \mathbf{A}^n$ *critical, parallelogram property*

Proof step 2: Similarity

Task: find short pp-definitions for $R \leq \mathbf{A}^n$ *critical, parallelogram property*
Strategy: as for $x_1 + x_2 + \ldots + x_n = a$

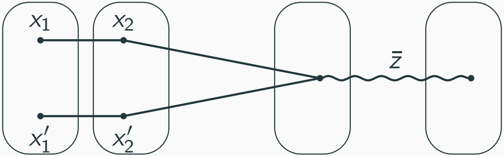
- $(x_1, x_2) \sim (x_1', x_2') :\Leftrightarrow \exists \bar{z}\, R(x_1, x_2, \bar{z}) \wedge R(x_1', x_2', \bar{z})$
- $\sim \in \mathrm{Con}(\mathrm{pr}_{1,2} R)$, $\mathbf{A}_{1,2} := (\mathrm{pr}_{1,2} R)/_\sim$

Proof step 2: Similarity

Task: find short pp-definitions for $R \leq \mathbf{A}^n$ *critical, parallelogram property*

Strategy: as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x_1', x_2') :\Leftrightarrow \exists \bar{z}\, R(x_1, x_2, \bar{z}) \wedge R(x_1', x_2', \bar{z})$
- $\sim \in \mathrm{Con}(\mathrm{pr}_{1,2} R)$, $\mathbf{A}_{1,2} := (\mathrm{pr}_{1,2} R)/_{\sim}$

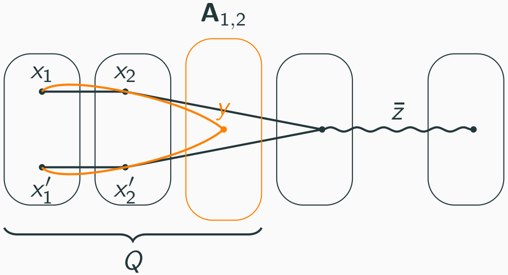


Proof step 2: Similarity

Task: find short pp-definitions for $R \leq \mathbf{A}^n$ *critical, parallelogram property*

Strategy: as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x_1', x_2') :\Leftrightarrow \exists \bar{z}\, R(x_1, x_2, \bar{z}) \wedge R(x_1', x_2', \bar{z})$
- $\sim \in \operatorname{Con}(\operatorname{pr}_{1,2} R)$, $\mathbf{A}_{1,2} := (\operatorname{pr}_{1,2} R)/_{\sim}$



$(x_1, x_2, y) \in Q :\Leftrightarrow$

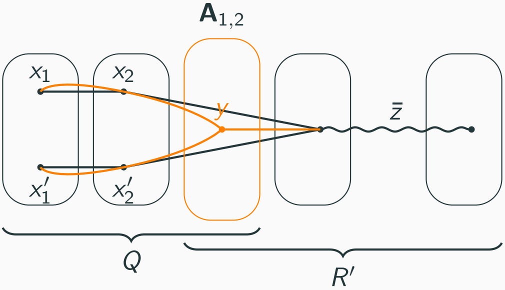
$y = (x_1, x_2)/_{\sim}$

Proof step 2: Similarity

Task: find short pp-definitions for $R \leq \mathbf{A}^n$ *critical, parallelogram property*

Strategy: as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x_1', x_2') :\Leftrightarrow \exists \bar{z}\, R(x_1, x_2, \bar{z}) \wedge R(x_1', x_2', \bar{z})$
- $\sim \in \mathrm{Con}(\mathrm{pr}_{1,2} R)$, $\mathbf{A}_{1,2} := (\mathrm{pr}_{1,2} R)/_\sim$



$(x_1, x_2, y) \in Q :\Leftrightarrow$
$y = (x_1, x_2)/_\sim$

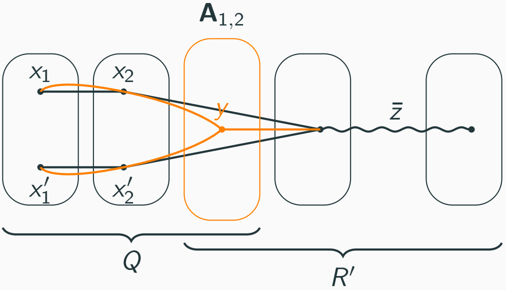
$(y, \bar{z}) \in R' :\Leftrightarrow$
$y = (x_1, x_2)/_\sim, (x_1, x_2, \bar{z}) \in R$

Proof step 2: Similarity

Task: find short pp-definitions for $R \leq \mathbf{A}^n$ *critical, parallelogram property*

Strategy: as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x_1', x_2') :\Leftrightarrow \exists \bar{z}\, R(x_1, x_2, \bar{z}) \wedge R(x_1', x_2', \bar{z})$
- $\sim \in \mathrm{Con}(\mathrm{pr}_{1,2} R)$, $\mathbf{A}_{1,2} := (\mathrm{pr}_{1,2} R)/_\sim$



$(x_1, x_2, y) \in Q :\Leftrightarrow$

$y = (x_1, x_2)/_\sim$

$(y, \bar{z}) \in R' :\Leftrightarrow$

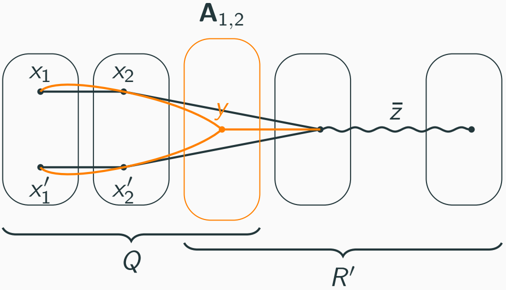
$y = (x_1, x_2)/_\sim, (x_1, x_2, \bar{z}) \in R$

$$R(x_1, x_2, x_3, \ldots, x_n) \Leftrightarrow \exists y \in A_{1,2}\, Q(x_1, x_2, y) \wedge R'(y, x_3, \ldots, x_n).$$

Proof step 2: Similarity

Task: find short pp-definitions for $R \leq \mathbf{A}^n$ *critical, parallelogram property*
Strategy: as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x_1', x_2') :\Leftrightarrow \exists \bar{z}\, R(x_1, x_2, \bar{z}) \wedge R(x_1', x_2', \bar{z})$
- $\sim \in \mathrm{Con}(\mathrm{pr}_{1,2} R)$, $\mathbf{A}_{1,2} := (\mathrm{pr}_{1,2} R)/_\sim$



$(x_1, x_2, y) \in Q :\Leftrightarrow$
$y = (x_1, x_2)/_\sim$

$(y, \bar{z}) \in R' :\Leftrightarrow$
$y = (x_1, x_2)/_\sim, (x_1, x_2, \bar{z}) \in R$

$$R(x_1, x_2, x_3, \ldots, x_n) \Leftrightarrow \exists y \in A_{1,2}\, Q(x_1, x_2, y) \wedge R'(y, x_3, \ldots, x_n).$$

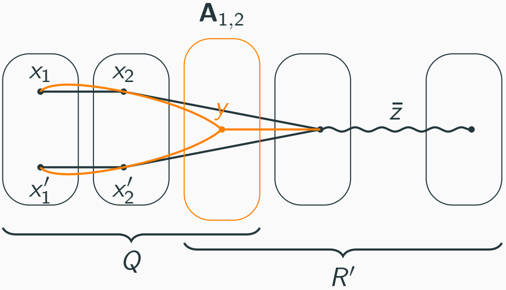
Problem: in general $\mathbf{A}_{1,2} \neq \mathbf{A}$

Proof step 2: Similarity

Task: find short pp-definitions for $R \leq \mathbf{A}^n$ *critical, parallelogram property*

Strategy: as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x_1', x_2') :\Leftrightarrow \exists \bar{z}\, R(x_1, x_2, \bar{z}) \wedge R(x_1', x_2', \bar{z})$
- $\sim \in \mathrm{Con}(\mathrm{pr}_{1,2} R)$, $\mathbf{A}_{1,2} := (\mathrm{pr}_{1,2} R)/_\sim$



$(x_1, x_2, y) \in Q :\Leftrightarrow$

$y = (x_1, x_2)/_\sim$

$(y, \bar{z}) \in R' :\Leftrightarrow$

$y = (x_1, x_2)/_\sim, (x_1, x_2, \bar{z}) \in R$

$$R(x_1, x_2, x_3, \ldots, x_n) \Leftrightarrow \exists y \in A_{1,2}\, Q(x_1, x_2, y) \wedge R'(y, x_3, \ldots, x_n).$$

Problem: in general $\mathbf{A}_{1,2} \neq \mathbf{A}$

But: R critical $\Rightarrow$ $\mathbf{A}_{1,2}$ is SI $\Rightarrow$ bounded by residual finiteness. $\square$

Application:
Subpower Membership Problem

Subpower Membership Problem

$\mathbf{A}$... finite algebra

SMP($\mathbf{A}$)
$\textsc{Input}$: $\bar{a}_1, \ldots, \bar{a}_k, \bar{b} \in A^n$
$\textsc{Decide}$: Is $\bar{b} \in \mathrm{Sg}_{\mathbf{A}^n}(\bar{a}_1, \ldots, \bar{a}_k)$?

Question (IMMVW'10): Is SMP($\mathbf{A}$) $\in$ P for $\mathbf{A}$ with few subpowers?

Subpower Membership Problem

A... finite algebra

SMP(**A**)
$\textsc{Input}$: $\bar{a}_1, \ldots, \bar{a}_k, \bar{b} \in A^n$
$\textsc{Decide}$: Is $\bar{b} \in \mathrm{Sg}_{\mathbf{A}^n}(\bar{a}_1, \ldots, \bar{a}_k)$?

Question (IMMVW'10): Is SMP(**A**) $\in$ P for **A** with few subpowers?

Observation
$\bar{b} \notin \mathrm{Sg}_{\mathbf{A}^n}(\bar{a}_1, \ldots, \bar{a}_k) \Leftrightarrow \exists$pp-fma.$\psi : \neg\psi(\bar{b}) \wedge \psi(\bar{a}_1) \wedge \ldots \wedge \psi(\bar{a}_k)$.
A has short pp-definitions $\Rightarrow$ SMP(**A**) $\in$ coNP.

Subpower Membership Problem

A... finite algebra

SMP(**A**)
Input: $\bar{a}_1, \ldots, \bar{a}_k, \bar{b} \in A^n$
Decide: Is $\bar{b} \in \mathrm{Sg}_{\mathbf{A}^n}(\bar{a}_1, \ldots, \bar{a}_k)$?

Question (IMMVW'10): Is SMP(**A**) $\in$ P for **A** with few subpowers?

Observation
$\bar{b} \notin \mathrm{Sg}_{\mathbf{A}^n}(\bar{a}_1, \ldots, \bar{a}_k) \Leftrightarrow \exists$pp-fma.$\psi : \neg\psi(\bar{b}) \wedge \psi(\bar{a}_1) \wedge \ldots \wedge \psi(\bar{a}_k)$.
A has short pp-definitions $\Rightarrow$ SMP(**A**) $\in$ coNP.

Theorem (BMS'19)

- SMP(**A**) $\in$ NP if **A** has few subpowers

(weak) Conjecture $\Rightarrow$ SMP(**A**) $\in$ NP $\cap$ coNP.

Subpower Membership Problem

A... finite algebra

SMP(**A**)
INPUT: $\bar{a}_1, \ldots, \bar{a}_k, \bar{b} \in A^n$
DECIDE: Is $\bar{b} \in \mathrm{Sg}_{\mathbf{A}^n}(\bar{a}_1, \ldots, \bar{a}_k)$?

Question (IMMVW'10): Is SMP(**A**) $\in$ P for **A** with few subpowers?

Observation
$\bar{b} \notin \mathrm{Sg}_{\mathbf{A}^n}(\bar{a}_1, \ldots, \bar{a}_k) \Leftrightarrow \exists$pp-fma.$\psi : \neg\psi(\bar{b}) \wedge \psi(\bar{a}_1) \wedge \ldots \wedge \psi(\bar{a}_k)$.
A has short pp-definitions $\Rightarrow$ SMP(**A**) $\in$ coNP.

Theorem (BMS'19)

- SMP(**A**) $\in$ NP if **A** has few subpowers
- SMP(**A**) $\in$ P if further HSP(**A**) is residually finite.

(weak) Conjecture $\Rightarrow$ SMP(**A**) $\in$ NP $\cap$ coNP.

Thank you for your attention!

Any questions?