The Complexity of Comparing Subalgebras Given by Generators

Ágnes Szendrei

Joint work with A. Bulatov and P. Mayr

AMS Western Sectional Meeting
Denver, CO, October 8–9, 2016

Two Decision Problems

$\mathcal{V}$: variety in a finite language
$\mathcal{K}$: finite set of finite algebras in $\mathcal{V}$

Two Decision Problems

$\mathcal{V}$: variety in a finite language
$\mathcal{K}$: finite set of finite algebras in $\mathcal{V}$

Comparing Subalgebras of Products in $\mathcal{K}$:

- INPUT: $b_1, \ldots, b_k, c_1, \ldots, c_\ell \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
- QUESTION: Is $\langle c_1, \ldots, c_\ell \rangle \leq \langle b_1, \ldots, b_k \rangle$?

Two Decision Problems

$\mathcal{V}$: variety in a finite language
$\mathcal{K}$: finite set of finite algebras in $\mathcal{V}$

Comparing Subalgebras of Products in $\mathcal{K}$:

- INPUT: $b_1, \ldots, b_k, c_1, \ldots, c_\ell \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
- QUESTION: Is $\langle c_1, \ldots, c_\ell \rangle \leq \langle b_1, \ldots, b_k \rangle$?

A polynomial time equivalent problem:

Subpower Membership Problem for $\mathcal{K}$, denoted $\mathrm{SMP}(\mathcal{K})$:

- INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
- QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Bad News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Bad News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Hard in general:

- SMP($\mathcal{K}$) $\in$ EXPTIME by naive algorithm

Bad News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Hard in general:

- $\mathrm{SMP}(\mathcal{K}) \in$ EXPTIME by naive algorithm
- $\exists$ finite $\mathbf{A}$ such that $\mathrm{SMP}(\mathbf{A})$ is EXPTIME-complete [Kozik, 2008]

Bad News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Hard in general:

- $\mathrm{SMP}(\mathcal{K}) \in$ EXPTIME by naive algorithm
- $\exists$ finite $\mathbf{A}$ such that $\mathrm{SMP}(\mathbf{A})$ is EXPTIME-complete [Kozik, 2008]

Complexity is not the property of the (generated) subvariety:

- $\mathrm{SMP}(\mathcal{K}) \quad = \quad \mathrm{SMP}(\mathbb{S}\mathcal{K})$

Bad News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Hard in general:

- SMP($\mathcal{K}$) $\in$ EXPTIME by naive algorithm
- $\exists$ finite $\mathbf{A}$ such that SMP($\mathbf{A}$) is EXPTIME-complete [Kozik, 2008]

Complexity is not the property of the (generated) subvariety:

- $\mathrm{SMP}(\mathcal{K}) \quad = \quad \mathrm{SMP}(\mathbb{S}\mathcal{K})$
- $\mathrm{SMP}(\mathcal{K}) \quad \overset{\text{poly time}}{\Longleftrightarrow} \quad \mathrm{SMP}(\mathbb{P}_{\leq m}\mathcal{K})$ for all $m \geq 1$.

Bad News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Hard in general:

- SMP($\mathcal{K}$) $\in$ EXPTIME by naive algorithm
- $\exists$ finite $\mathbf{A}$ such that SMP($\mathbf{A}$) is EXPTIME-complete [Kozik, 2008]

Complexity is not the property of the (generated) subvariety:

- $\mathrm{SMP}(\mathcal{K}) \;=\; \mathrm{SMP}(\mathbb{S}\mathcal{K})$
- $\mathrm{SMP}(\mathcal{K}) \overset{\text{poly time}}{\Longleftrightarrow} \mathrm{SMP}(\mathbb{P}_{\leq m}\mathcal{K})$ for all $m \geq 1$.
- $\mathrm{SMP}(\mathcal{K}) \overset{\text{poly time}}{\not\Longleftrightarrow} \mathrm{SMP}(\mathbb{H}\mathcal{K})$

Bad News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Hard in general:

- SMP($\mathcal{K}$) $\in$ EXPTIME by naive algorithm
- $\exists$ finite $\mathbf{A}$ such that SMP($\mathbf{A}$) is EXPTIME-complete [Kozik, 2008]

Complexity is not the property of the (generated) subvariety:

- $\mathrm{SMP}(\mathcal{K}) \quad = \quad \mathrm{SMP}(\mathbb{S}\mathcal{K})$
- $\mathrm{SMP}(\mathcal{K}) \overset{\text{poly time}}{\Longleftrightarrow} \mathrm{SMP}(\mathbb{P}_{\leq m}\mathcal{K})$ for all $m \geq 1$.
- $\mathrm{SMP}(\mathcal{K}) \overset{\text{poly time}}{\not\Longleftrightarrow} \mathrm{SMP}(\mathbb{H}\mathcal{K})$
  - $\exists$ 10-element semigroup $\mathbf{S}$ and a 9-element homomorphic image $\bar{\mathbf{S}}$ of $\mathbf{S}$ such that SMP($\mathbf{S}$) $\in$ P while SMP($\bar{\mathbf{S}}$) is NP-complete [Steindl, ∼2016]

Good News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Good News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Easy (lies in P) in many 'classical' varieties:

- vector spaces – use Gaussian elimination

Good News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Easy (lies in P) in many 'classical' varieties:

- vector spaces – use Gaussian elimination
- groups – Sim's Algorithm [$\approx$ 1970]

Good News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Easy (lies in P) in many 'classical' varieties:

- vector spaces – use Gaussian elimination
- groups – Sim's Algorithm [$\approx$ 1970]
- NU varieties – based on the Baker–Pixley Theorem [1975]

Good News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Easy (lies in P) in many 'classical' varieties:

- vector spaces – use Gaussian elimination
- groups – Sim's Algorithm [$\approx$ 1970]
- NU varieties – based on the Baker–Pixley Theorem [1975]
- groups expanded by multilinear operations (including rings, modules, ...) – adapt Sim's Algorithm [Willard, 2007]

Good News

SMP($\mathcal{K}$): INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Easy (lies in P) in many 'classical' varieties:

- vector spaces – use Gaussian elimination
- groups – Sim's Algorithm [$\approx$ 1970]
- NU varieties – based on the Baker–Pixley Theorem [1975]
- groups expanded by multilinear operations (including rings, modules, ...) – adapt Sim's Algorithm [Willard, 2007]
- expansions of nilpotent Mal'tsev algebras of order p^k [Mayr, 2012]

Good News

$\mathrm{SMP}(\mathcal{K})$: INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$.
QUESTION: Is $c \in \langle b_1, \ldots, b_k \rangle$?

Easy (lies in P) in many 'classical' varieties:

- vector spaces – use Gaussian elimination
- groups – Sim's Algorithm [$\approx$ 1970]
- NU varieties – based on the Baker–Pixley Theorem [1975]
- groups expanded by multilinear operations (including rings, modules, ...) – adapt Sim's Algorithm [Willard, 2007]
- expansions of nilpotent Mal'tsev algebras of order p^k [Mayr, 2012]

Problem. Is $\mathrm{SMP}(\mathbf{A}) \in \mathsf{P}$ whenever $\mathcal{V}(\mathbf{A})$ has a Mal'tsev/cube term?
[Willard, 2007]/[IMMVW, 2010]

Cube Terms

Definition. A *d-cube term* ($d \geq 2$) for a class $\mathcal{K}$ of algebras is a term C s.t.

$$\mathcal{K} \models C\Bigg(\underbrace{\begin{bmatrix} x \\ y \\ \vdots \\ y \end{bmatrix}, \begin{bmatrix} y \\ x \\ \vdots \\ y \end{bmatrix}, \ldots, \begin{bmatrix} y \\ y \\ \vdots \\ x \end{bmatrix}, \begin{bmatrix} x \\ x \\ \vdots \\ y \end{bmatrix}, \ldots}_{d\text{-tuples in } x,\, y, \text{ with at least one } x}\Bigg) = \begin{bmatrix} y \\ y \\ \vdots \\ y \end{bmatrix}.$$

Cube Terms

Definition. A *d-cube term* ($d \geq 2$) for a class $\mathcal{K}$ of algebras is a term C s.t.

$$\mathcal{K} \models C\Bigg(\underbrace{\begin{bmatrix} x \\ y \\ \vdots \\ y \end{bmatrix}, \begin{bmatrix} y \\ x \\ \vdots \\ y \end{bmatrix}, \dots, \begin{bmatrix} y \\ y \\ \vdots \\ x \end{bmatrix}, \begin{bmatrix} x \\ x \\ \vdots \\ y \end{bmatrix}, \dots}_{d\text{-tuples in } x,\, y, \text{ with at least one } x}\Bigg) = \begin{bmatrix} y \\ y \\ \vdots \\ y \end{bmatrix}.$$

Examples. Mal'tsev term, near unanimity term

Cube Terms

Definition. A *d-cube term* ($d \geq 2$) for a class $\mathcal{K}$ of algebras is a term C s.t.

$$\mathcal{K} \models C\left(\underbrace{\begin{bmatrix} x \\ y \\ \vdots \\ y \end{bmatrix}, \begin{bmatrix} y \\ x \\ \vdots \\ y \end{bmatrix}, \ldots, \begin{bmatrix} y \\ y \\ \vdots \\ x \end{bmatrix}, \begin{bmatrix} x \\ x \\ \vdots \\ y \end{bmatrix}, \ldots}_{d\text{-tuples in } x,\, y, \text{ with at least one } x}\right) = \begin{bmatrix} y \\ y \\ \vdots \\ y \end{bmatrix}.$$

Examples. Mal'tsev term, near unanimity term

For a finite algebra **A**,

- **A** has a cube term $\Leftrightarrow$ **A** has *few subpowers*, i.e.
  $\diamond$ $\log_2 |\mathrm{Sub}(\mathbf{A}^n)| \leq \text{const} \cdot n^k$ for some k

  [Berman, Idziak, Marković, McKenzie, Valeriote, Willard, 2010]

Cube Terms

Definition. A *d-cube term* ($d \geq 2$) for a class $\mathcal{K}$ of algebras is a term C s.t.

$$\mathcal{K} \models C\left(\underbrace{\begin{bmatrix} x \\ y \\ \vdots \\ y \end{bmatrix}, \begin{bmatrix} y \\ x \\ \vdots \\ y \end{bmatrix}, \ldots, \begin{bmatrix} y \\ y \\ \vdots \\ x \end{bmatrix}, \begin{bmatrix} x \\ x \\ \vdots \\ y \end{bmatrix}, \ldots}_{d\text{-tuples in } x,\, y, \text{ with at least one } x}\right) = \begin{bmatrix} y \\ y \\ \vdots \\ y \end{bmatrix}.$$

Examples. Mal'tsev term, near unanimity term

For a finite algebra $\mathbf{A}$,

- ($\mathcal{V}(\mathbf{A})$ CM $\Leftarrow$) $\mathbf{A}$ has a cube term $\Leftrightarrow$ $\mathbf{A}$ has *few subpowers*, i.e.
  $\diamond$ $\log_2 |\mathrm{Sub}(\mathbf{A}^n)| \leq \mathrm{const} \cdot n^k$ for some k

  [Berman, Idziak, Marković, McKenzie, Valeriote, Willard, 2010]

Cube Terms

Definition. A *d-cube term* ($d \geq 2$) for a class $\mathcal{K}$ of algebras is a term C s.t.

$$\mathcal{K} \models C\Bigg(\underbrace{\begin{bmatrix} x \\ y \\ \vdots \\ y \end{bmatrix}, \begin{bmatrix} y \\ x \\ \vdots \\ y \end{bmatrix}, \ldots, \begin{bmatrix} y \\ y \\ \vdots \\ x \end{bmatrix}, \begin{bmatrix} x \\ x \\ \vdots \\ y \end{bmatrix}, \ldots}_{d\text{-tuples in } x,\, y, \text{ with at least one } x}\Bigg) = \begin{bmatrix} y \\ y \\ \vdots \\ y \end{bmatrix}.$$

Examples. Mal'tsev term, near unanimity term

For a finite algebra $\mathbf{A}$,

- ($\mathcal{V}(\mathbf{A})$ CM $\Leftarrow$) $\mathbf{A}$ has a cube term $\Leftrightarrow$ $\mathbf{A}$ has *few subpowers*, i.e.
  $\diamond$ $\log_2 |\mathrm{Sub}(\mathbf{A}^n)| \leq \mathrm{const} \cdot n^k$ for some k
  [Berman, Idziak, Marković, McKenzie, Valeriote, Willard, 2010]
- $\mathbf{A}$ has a cube term $\Rightarrow$ $\mathbf{A}$ is *finitely related*
  [Aichinger, Mayr, McKenzie, 2014]

Cube Terms

Definition. A *d-cube term* ($d \geq 2$) for a class $\mathcal{K}$ of algebras is a term C s.t.

$$\mathcal{K} \models C\Bigg(\underbrace{\begin{bmatrix} x \\ y \\ \vdots \\ y \end{bmatrix}, \begin{bmatrix} y \\ x \\ \vdots \\ y \end{bmatrix}, \ldots, \begin{bmatrix} y \\ y \\ \vdots \\ x \end{bmatrix}, \begin{bmatrix} x \\ x \\ \vdots \\ y \end{bmatrix}, \ldots}_{d\text{-tuples in } x,\, y,\text{ with at least one } x}\Bigg) = \begin{bmatrix} y \\ y \\ \vdots \\ y \end{bmatrix}.$$

Examples. Mal'tsev term, near unanimity term

For a finite algebra $\mathbf{A}$,

- $(\mathcal{V}(\mathbf{A})$ CM $\Leftarrow)$ $\mathbf{A}$ has a cube term $\Leftrightarrow$ $\mathbf{A}$ has *few subpowers*, i.e.
  $\diamond$ $\log_2 |\mathrm{Sub}(\mathbf{A}^n)| \leq \mathrm{const} \cdot n^k$ for some k
  [Berman, Idziak, Marković, McKenzie, Valeriote, Willard, 2010]
- $\mathbf{A}$ has a cube term $\Rightarrow$ $\mathbf{A}$ is *finitely related*
  [Aichinger, Mayr, McKenzie, 2014]
- $\mathbf{A}$ finitely related & $\mathcal{V}(\mathbf{A})$ CM $\Rightarrow$ $\mathbf{A}$ has a cube term [Barto, ∼2016]

SMP($\mathcal{K}$): An Application in AI

Learnability

SMP($\mathcal{K}$): An Application in AI

Learnability

- Let $\mathbf{A} = (A, C)$ be a finite algebra with a cube operation C

SMP($\mathcal{K}$): An Application in AI

Learnability

- Let $\mathbf{A} = (A, C)$ be a finite algebra with a cube operation C
- Set of 'concepts' to be learned: $\Gamma = \bigcup_k \mathrm{Sub}(\mathbf{A}^k)$, each $S \in \Gamma$ encoded by its compact representation (a special generating set)

SMP($\mathcal{K}$): An Application in AI

Learnability

- Let $\mathbf{A} = (A, C)$ be a finite algebra with a cube operation C
- Set of 'concepts' to be learned: $\Gamma = \bigcup_k \mathrm{Sub}(\mathbf{A}^k)$, each $S \in \Gamma$ encoded by its compact representation (a special generating set)
- Learning model: 'Exact learning with equivalence queries'
  - Algorithm provides oracle with a hypothetical encoding e of a concept S
  - The oracle either confirms that e encodes S, or it returns a counterexample from the symmetric difference of S and the concept encoded by e.

SMP($\mathcal{K}$): An Application in AI

Learnability

- Let $\mathbf{A} = (A, C)$ be a finite algebra with a cube operation C
- Set of 'concepts' to be learned: $\Gamma = \bigcup_k \mathrm{Sub}(\mathbf{A}^k)$, each $S \in \Gamma$ encoded by its compact representation (a special generating set)
- Learning model: 'Exact learning with equivalence queries'
  - Algorithm provides oracle with a hypothetical encoding e of a concept S
  - The oracle either confirms that e encodes S, or it returns a counterexample from the symmetric difference of S and the concept encoded by e.
- Γ *is polynomially exactly learnable with equivalence queries.* [Idziak, Marković, McKenzie, Valeriote, Willard, 2010]
  - Generalizes [Dalmau, Jeavons, 2003] and [Bulatov, Chen, Dalmau, 2007]

SMP($\mathcal{K}$): An Application in AI

Learnability

- Let $\mathbf{A} = (A, C)$ be a finite algebra with a cube operation C
- Set of 'concepts' to be learned: $\Gamma = \bigcup_k \mathrm{Sub}(\mathbf{A}^k)$, each $S \in \Gamma$ encoded by its compact representation (a special generating set)
- Learning model: 'Exact learning with equivalence queries'
  - Algorithm provides oracle with a hypothetical encoding e of a concept S
  - The oracle either confirms that e encodes S, or it returns a counterexample from the symmetric difference of S and the concept encoded by e.
- Γ *is polynomially exactly learnable with equivalence queries.* [Idziak, Marković, McKenzie, Valeriote, Willard, 2010]
  - Generalizes [Dalmau, Jeavons, 2003] and [Bulatov, Chen, Dalmau, 2007]
- $\mathrm{SMP}(\mathbf{A}) \in \mathsf{P}$ would yield a more direct aproach (and cleaner proof).

Main Results

Theorem

If $\mathcal{V}$ has a cube term, then for every finite $\mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$ the following problems are all polynomial time equivalent, and are in NP*:*

- *Given $b_1, \ldots, b_k \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$, find a compact representation for $\langle b_1, \ldots, b_k \rangle$.*
- $\mathrm{SMP}(\mathcal{K})$.
- $\mathrm{SMP}(\mathbb{H}\mathcal{K})$.

Main Results

Theorem

If $\mathcal{V}$ has a cube term, then for every finite $\mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$ the following problems are all polynomial time equivalent, and are in NP*:*

- *Given $b_1, \ldots, b_k \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$, find a compact representation for $\langle b_1, \ldots, b_k \rangle$.*
- $\mathrm{SMP}(\mathcal{K})$.
- $\mathrm{SMP}(\mathbb{H}\mathcal{K})$.

We don't know whether these problems are in P. However, we have:

Main Results

Theorem

If $\mathcal{V}$ has a cube term, then for every finite $\mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$ the following problems are all polynomial time equivalent, and are in NP*:*

- *Given $b_1, \ldots, b_k \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$, find a compact representation for $\langle b_1, \ldots, b_k \rangle$.*
- $\mathrm{SMP}(\mathcal{K})$.
- $\mathrm{SMP}(\mathbb{H}\mathcal{K})$.

We don't know whether these problems are in P. However, we have:

Theorem

If $\mathcal{V}$ is a residually small variety with a cube term, then

$$\mathrm{SMP}(\mathcal{K}) \in \mathsf{P} \qquad \textit{for every finite } \mathcal{K} \subseteq \mathcal{V}_{\text{fin}}.$$

Main Results

Theorem

If $\mathcal{V}$ has a cube term, then for every finite $\mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$ the following problems are all polynomial time equivalent, and are in NP*:*

- *Given $b_1, \ldots, b_k \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$, find a compact representation for $\langle b_1, \ldots, b_k \rangle$.*
- $\mathrm{SMP}(\mathcal{K})$.
- $\mathrm{SMP}(\mathbb{H}\mathcal{K})$.

Proof uses compact representations.

We don't know whether these problems are in P. However, we have:

Theorem

If $\mathcal{V}$ is a residually small variety with a cube term, then

$$\mathrm{SMP}(\mathcal{K}) \in \mathsf{P} \qquad \textit{for every finite } \mathcal{K} \subseteq \mathcal{V}_{\text{fin}}.$$

Main Results

Theorem

If $\mathcal{V}$ has a cube term, then for every finite $\mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$ the following problems are all polynomial time equivalent, and are in NP*:*

- *Given $b_1, \ldots, b_k \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ with $\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K}$, find a compact representation for $\langle b_1, \ldots, b_k \rangle$.*
- $\mathrm{SMP}(\mathcal{K})$.
- $\mathrm{SMP}(\mathbb{H}\mathcal{K})$.

Proof uses compact representations.

We don't know whether these problems are in P. However, we have:

Theorem

If $\mathcal{V}$ is a residually small variety with a cube term, then

$$\mathrm{SMP}(\mathcal{K}) \in \mathsf{P} \qquad \textit{for every finite } \mathcal{K} \subseteq \mathcal{V}_{\text{fin}}.$$

Proof uses structure theorem for subalgebras of products [Kearnes–Sz, 2012].

Idea of Proof of 2nd Theorem

INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ $(\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}})$

Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ $(\mathbf{B}_i \leq \mathbf{A}_i)$

Idea of Proof of 2nd Theorem

INPUT: $b_1, \dots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ $(\mathbf{A}_1, \dots, \mathbf{A}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}})$

Let $\mathbf{B} := \langle b_1, \dots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ $(\mathbf{B}_i \leq \mathbf{A}_i)$

QUESTION: Is $c \in \mathbf{B}$?

Idea of Proof of 2nd Theorem

INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ $(\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}})$

Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ $(\mathbf{B}_i \leq \mathbf{A}_i)$

QUESTION: Is $c \in \mathbf{B}$?

May assume:

- $\mathcal{V}$ has a d-cube term;

Idea of Proof of 2nd Theorem

INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ $(\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}})$

Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ $(\mathbf{B}_i \leq \mathbf{A}_i)$

QUESTION: Is $c \in \mathbf{B}$?

May assume:

- $\mathcal{V}$ has a d-cube term;
- $\mathbb{HS}\mathcal{K} \subseteq \mathcal{K}$;

Idea of Proof of 2nd Theorem

INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ $(\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}})$

Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ $(\mathbf{B}_i \leq \mathbf{A}_i)$

QUESTION: Is $c \in \mathbf{B}$?

May assume:

- $\mathcal{V}$ has a d-cube term;
- $\mathbb{HS}\mathcal{K} \subseteq \mathcal{K}$;
- $c|_I \in \mathbf{B}|_I = \langle b_1|_I, \ldots, b_k|_I \rangle$ for all $I \in \binom{[n]}{d}$;

Idea of Proof of 2nd Theorem

INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ $(\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}})$

Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ $(\mathbf{B}_i \leq \mathbf{A}_i)$

QUESTION: Is $c \in \mathbf{B}$?

May assume:

- $\mathcal{V}$ has a d-cube term;
- $\mathbb{HS}\mathcal{K} \subseteq \mathcal{K}$;
- $c|_I \in \mathbf{B}|_I = \langle b_1|_I, \ldots, b_k|_I \rangle$ for all $I \in \binom{[n]}{d}$;
- in particular, $c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$;

Idea of Proof of 2nd Theorem

INPUT: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ $(\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}})$

Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ $(\mathbf{B}_i \leq \mathbf{A}_i)$

QUESTION: Is $c \in \mathbf{B}$?

May assume:

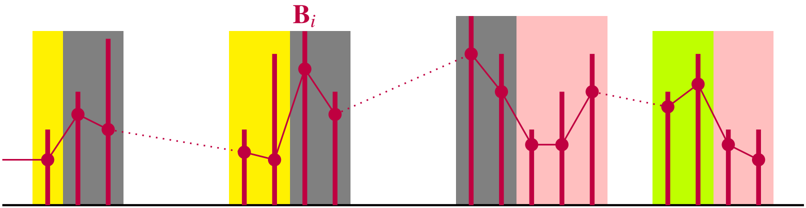
- $\mathcal{V}$ has a d-cube term;
- $\mathbb{H}\mathbb{S}\mathcal{K} \subseteq \mathcal{K}$;
- $c|_I \in \mathbf{B}|_I = \langle b_1|_I, \ldots, b_k|_I \rangle$ for all $I \in \binom{[n]}{d}$;
- in particular, $c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$;
- $\mathbf{B}_1, \ldots, \mathbf{B}_n$ are subdirectly irreducible.

Idea of Proof (Cont'd)

Structure Theorem $\Rightarrow$

Structure Theorem $\Rightarrow$

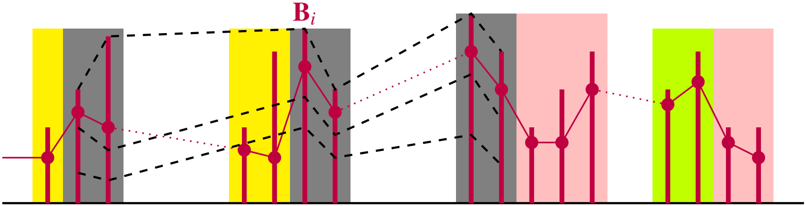
- we have an equivalence relation $\sim$ on $[n] = \{1, \ldots, n\}$ (indexing the coordinates) such that
  - $i \sim j$ iff $i = j$ or $\mathbf{B}_i$, $\mathbf{B}_j$ are similar SIs with abelian monoliths μ_i, μ_j, and



Idea of Proof (Cont'd)

Structure Theorem $\Rightarrow$

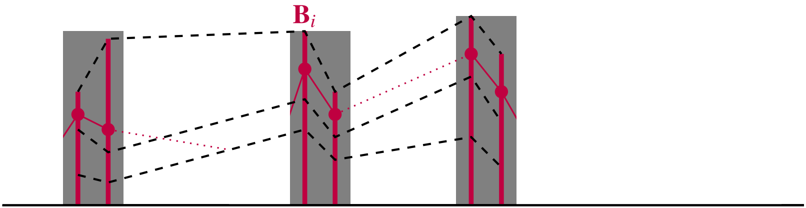
- we have an equivalence relation $\sim$ on $[n] = \{1, \ldots, n\}$ (indexing the coordinates) such that
  - $i \sim j$ iff $i = j$ or $\mathbf{B}_i$, $\mathbf{B}_j$ are similar SIs with abelian monoliths μ_i, μ_j, and
  - for the centralizers $\rho_i = (0 : \mu_i)$, $\rho_j = (0 : \mu_j)$, $\mathbf{B}|_{i,j}/(\rho_i \times \rho_j)$ is the graph of an isomorphism $\mathbf{B}_i/\rho_i \to \mathbf{B}_j/\rho_j$.



Idea of Proof (Cont'd)

Structure Theorem ⇒

- we have an equivalence relation $\sim$ on $[n] = \{1, \ldots, n\}$ (indexing the coordinates) such that
  - $i \sim j$ iff $i = j$ or $\mathbf{B}_i$, $\mathbf{B}_j$ are similar SIs with abelian monoliths μ_i, μ_j, and
  - for the centralizers $\rho_i = (0 : \mu_i)$, $\rho_j = (0 : \mu_j)$, $\mathbf{B}|_{i,j}/(\rho_i \times \rho_j)$ is the graph of an isomorphism $\mathbf{B}_i/\rho_i \to \mathbf{B}_j/\rho_j$.



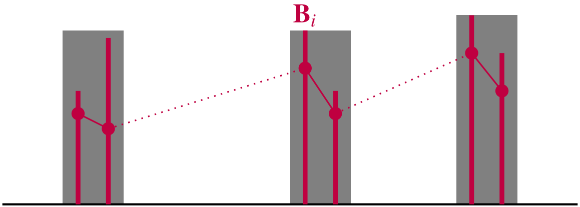
- $c \in \mathbf{B}$ iff $c|_U \in \mathbf{B}|_U$ for all blocks U $(\subseteq [n])$ of $\sim$ of size $|U| \geq \max\{d, 3\}$.

Idea of Proof (Cont'd)

$\mathcal{V}$ residually small $\Rightarrow$

Idea of Proof (Cont'd)

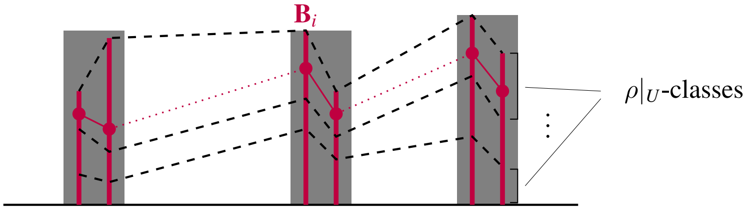
$\mathcal{V}$ residually small $\Rightarrow$ for every U,



Idea of Proof (Cont'd)

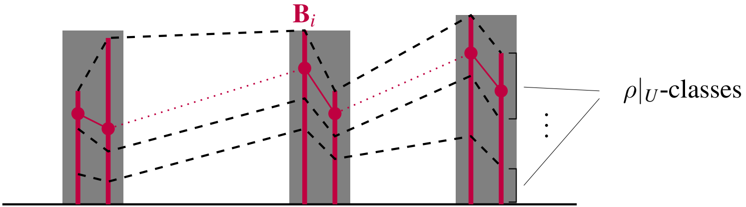
$\mathcal{V}$ residually small $\Rightarrow$ for every U,

- $\rho|_U = \prod_{i \in U} \rho_i$ is an abelian congruence on $\mathbf{B}|_U$, and



$\mathcal{V}$ residually small $\Rightarrow$ for every U,

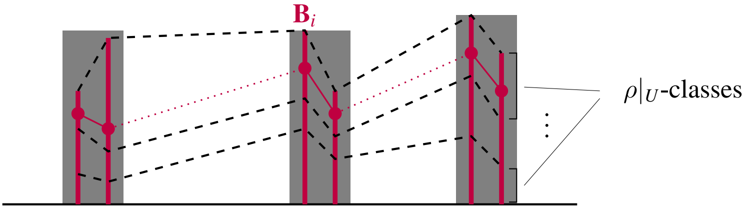
- $\rho|_U = \prod_{i\in U} \rho_i$ is an abelian congruence on $\mathbf{B}|_U$, and $\rho|_U$ has a bounded number of classes on $\mathbf{B}|_U$



Idea of Proof (Cont'd)

$\mathcal{V}$ residually small $\Rightarrow$ for every U,

- $\rho|_U = \prod_{i \in U} \rho_i$ is an abelian congruence on $\mathbf{B}|_U$, and $\rho|_U$ has a bounded number of classes on $\mathbf{B}|_U$

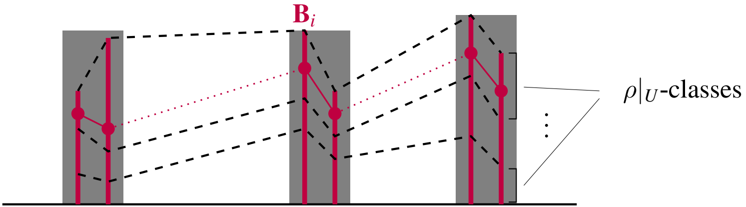


- a term induces a ternary abelian group op. $x - y + z$ on each ρ-class, and

Idea of Proof (Cont'd)

$\mathcal{V}$ residually small $\Rightarrow$ for every U,

- $\rho|_U = \prod_{i \in U} \rho_i$ is an abelian congruence on $\mathbf{B}|_U$, and $\rho|_U$ has a bounded number of classes on $\mathbf{B}|_U$

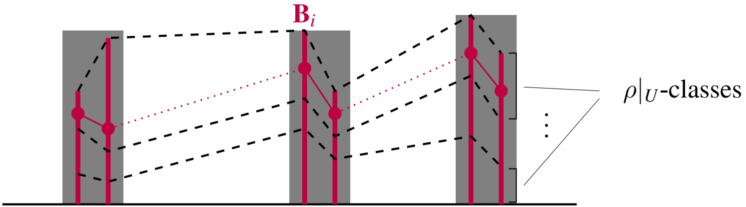


- a term induces a ternary abelian group op. $x - y + z$ on each ρ-class, and
- the sum of the ρ-classes is (essentially) a module ${}_R\mathbf{M}$ for a finite ring R that depends only on $\mathcal{K}$

Idea of Proof (Cont'd)

$\mathcal{V}$ residually small $\Rightarrow$ for every U,

- $\rho|_U = \prod_{i\in U} \rho_i$ is an abelian congruence on $\mathbf{B}|_U$, and $\rho|_U$ has a bounded number of classes on $\mathbf{B}|_U$



- a term induces a ternary abelian group op. $x - y + z$ on each ρ-class, and
- the sum of the ρ-classes is (essentially) a module ${}_R\mathbf{M}$ for a finite ring R that depends only on $\mathcal{K}$

- $\mathrm{SMP}({}_R\mathbf{M}) \in \mathsf{P} \;\Rightarrow\; \mathrm{SMP}(\mathcal{K}) \in \mathsf{P}$.