The Subpower Membership Problem for Finite Algebras with Cube Terms

Ágnes Szendrei

Joint work with A. Bulatov and P. Mayr

Algebra and Algorithms
Boulder, CO, May 19–22, 2016

Main Result

$\boxed{\text{Algebras}}$ $\boxed{\text{Algorithms}}$

$\boxed{\text{Structure}}$ $\boxed{\text{Complexity}}$

Main Result

Algebras

Algorithms

$\mathcal{V}$: variety in a finite language

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

Structure

Complexity

Algebras

Algorithms

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

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 $c \in \langle b_1, \ldots, b_k \rangle$?

Structure

Complexity

Main Result

Algebras

Algorithms

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

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 $c \in \langle b_1, \ldots, b_k \rangle$?

Theorem

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

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

Structure

Complexity

Cube Terms

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

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

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

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 **A**,

- **A** has a cube term $\Leftrightarrow$ **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]

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($\mathcal{K}$): What Do we Know?

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 $c \in \langle b_1, \ldots, b_k \rangle$?

SMP($\mathcal{K}$): What Do we Know?

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

SMP($\mathcal{K}$): What Do we Know?

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]

SMP($\mathcal{K}$): What Do we Know?

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:

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

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

- vector spaces – use Gaussian elimination

SMP($\mathcal{K}$): What Do we Know?

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]

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

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

SMP($\mathcal{K}$): What Do we Know?

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:

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

Easy (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]

SMP($\mathcal{K}$): What Do we Know?

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]

Easy (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]

SMP($\mathcal{K}$): What Do we Know?

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

Hard in general:

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

Easy (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]

SMP($\mathcal{K}$): What Do we Know?

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:

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

Easy (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]

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 simpler proof.

SMP for $\mathcal{K}$ v. $\mathbb{H}\mathcal{K}$, $\mathbb{S}\mathcal{K}$, $\mathbb{P}_{\leq m}\mathcal{K}$

SMP for $\mathcal{K}$ v. $\mathbb{H}\mathcal{K}$, $\mathbb{S}\mathcal{K}$, $\mathbb{P}_{\leq m}\mathcal{K}$

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

SMP for $\mathcal{K}$ v. $\mathbb{H}\mathcal{K}$, $\mathbb{S}\mathcal{K}$, $\mathbb{P}_{\leq m}\mathcal{K}$

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

SMP for $\mathcal{K}$ v. $\mathbb{H}\mathcal{K}$, $\mathbb{S}\mathcal{K}$, $\mathbb{P}_{\leq m}\mathcal{K}$

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

SMP for $\mathcal{K}$ v. $\mathbb{H}\mathcal{K}$, $\mathbb{S}\mathcal{K}$, $\mathbb{P}_{\leq m}\mathcal{K}$

- $\mathrm{SMP}(\mathcal{K}) \quad = \quad \mathrm{SMP}(\mathbb{S}\mathcal{K})$
- $\mathrm{SMP}(\mathcal{K}) \quad \overset{\text{poly time}}{\Longleftrightarrow} \quad \mathrm{SMP}(\mathbb{P}_{\leq m}\mathcal{K})$ for all $m \geq 1$.
- $\mathrm{SMP}(\mathcal{K}) \quad \overset{\text{poly time}}{\not\Longleftrightarrow} \quad \mathrm{SMP}(\mathbb{H}\mathcal{K})$
  - $\exists$ 10-element semigroup $\mathbf{S}$ and a 9-element homomorphic image $\bar{\mathbf{S}}$ of $\mathbf{S}$ such that $\mathrm{SMP}(\mathbf{S}) \in \mathsf{P}$ while $\mathrm{SMP}(\bar{\mathbf{S}})$ is NP-complete [Steindl, 2017?]

SMP for $\mathcal{K}$ v. $\mathbb{H}\mathcal{K}$, $\mathbb{S}\mathcal{K}$, $\mathbb{P}_{\leq m}\mathcal{K}$

- $\mathrm{SMP}(\mathcal{K}) \quad = \quad \mathrm{SMP}(\mathbb{S}\mathcal{K})$
- $\mathrm{SMP}(\mathcal{K}) \quad \overset{\text{poly time}}{\Longleftrightarrow} \quad \mathrm{SMP}(\mathbb{P}_{\leq m}\mathcal{K})$ for all $m \geq 1$.
- $\mathrm{SMP}(\mathcal{K}) \quad \overset{\text{poly time}}{\not\Longleftrightarrow} \quad \mathrm{SMP}(\mathbb{H}\mathcal{K})$
  - $\exists$ 10-element semigroup $\mathbf{S}$ and a 9-element homomorphic image $\bar{\mathbf{S}}$ of $\mathbf{S}$ such that $\mathrm{SMP}(\mathbf{S}) \in \mathsf{P}$ while $\mathrm{SMP}(\bar{\mathbf{S}})$ is NP-complete [Steindl, 2017?]

However:

Theorem

If $\mathcal{V}$ has a cube term, then for every finite $\mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$ we have that

$$\mathrm{SMP}(\mathcal{K}) \quad \overset{\text{poly time}}{\Longleftrightarrow} \quad \mathrm{SMP}(\mathbb{H}\mathcal{K}).$$

Critical Algebras in Varieties with a Cube Term: Reduction

Let $\mathcal{V}$ be a variety with a d-cube term.

Critical Algebras in Varieties with a Cube Term: Reduction

Let $\mathcal{V}$ be a variety with a d-cube term.
Let $\mathbf{R} \leq_{\text{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$.

Critical Algebras in Varieties with a Cube Term: Reduction

Let $\mathcal{V}$ be a variety with a d-cube term.
Let $\mathbf{R} \leq_{\mathrm{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$.

- Assume $\mathbf{R}$ is a *critical subalgebra* of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$, that is,
  - $\mathbf{R}$ is completely $\cap$-irreducible in $\mathrm{Sub}(\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)$, and
  - $\mathbf{R}$ is *directly indecomposable*, i.e., $[n]$ has no partition $\{I, J\}$ such that $\mathbf{R}$ and $\mathbf{R}|_I \times \mathbf{R}|_J$ differ only by a permutation of coordinates.

Critical Algebras in Varieties with a Cube Term: Reduction

Let $\mathcal{V}$ be a variety with a d-cube term.
Let $\mathbf{R} \leq_{\text{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$.

- Assume $\mathbf{R}$ is a *critical subalgebra* of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$, that is,
  - $\mathbf{R}$ is completely $\cap$-irreducible in $\mathrm{Sub}(\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)$, and
  - $\mathbf{R}$ is *directly indecomposable*, i.e., $[n]$ has no partition $\{I, J\}$ such that $\mathbf{R}$ and $\mathbf{R}|_I \times \mathbf{R}|_J$ differ only by a permutation of coordinates.
- Let $\theta = \theta_1 \times \cdots \times \theta_n$ ($\theta_i \in \mathrm{Con}(\mathbf{R}_i)$) be the largest product congruence of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ such that $\mathbf{R}$ is *θ-saturated*, i.e.,

Critical Algebras in Varieties with a Cube Term: Reduction

Let $\mathcal{V}$ be a variety with a d-cube term.
Let $\mathbf{R} \leq_{\mathrm{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$.

- Assume $\mathbf{R}$ is a *critical subalgebra* of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$, that is,
  - $\mathbf{R}$ is completely $\cap$-irreducible in $\mathrm{Sub}(\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)$, and
  - $\mathbf{R}$ is *directly indecomposable*, i.e., $[n]$ has no partition $\{I, J\}$ such that $\mathbf{R}$ and $\mathbf{R}|_I \times \mathbf{R}|_J$ differ only by a permutation of coordinates.
- Let $\theta = \theta_1 \times \cdots \times \theta_n$ ($\theta_i \in \mathrm{Con}(\mathbf{R}_i)$) be the largest product congruence of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ such that $\mathbf{R}$ is *θ-saturated*, i.e.,

$$\begin{array}{ccccc}
 & \mathbf{R} & \hookrightarrow & \mathbf{R}_1 \times \cdots \times \mathbf{R}_n & \\
 & \downarrow{\scriptstyle \nu_\theta} & & \downarrow{\scriptstyle \nu_{\theta_1}} \qquad\quad \downarrow{\scriptstyle \nu_{\theta_n}} & \\
\mathbf{R}/\theta|_{\mathbf{R}} = & \overline{\mathbf{R}} & \hookrightarrow & \overline{\mathbf{R}}_1 \times \cdots \times \overline{\mathbf{R}}_n & \cong (\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)/\theta
\end{array}$$

Critical Algebras in Varieties with a Cube Term: Reduction

Let $\mathcal{V}$ be a variety with a d-cube term.
Let $\mathbf{R} \leq_{\text{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$.

- Assume $\mathbf{R}$ is a *critical subalgebra* of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$, that is,
  - $\mathbf{R}$ is completely $\cap$-irreducible in $\text{Sub}(\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)$, and
  - $\mathbf{R}$ is *directly indecomposable*, i.e., $[n]$ has no partition $\{I, J\}$ such that $\mathbf{R}$ and $\mathbf{R}|_I \times \mathbf{R}|_J$ differ only by a permutation of coordinates.
- Let $\theta = \theta_1 \times \cdots \times \theta_n$ ($\theta_i \in \text{Con}(\mathbf{R}_i)$) be the largest product congruence of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ such that $\mathbf{R}$ is *θ-saturated*, i.e.,

$$\begin{array}{ccccc} (\nu_{\theta_1} \times \ldots \times \nu_{\theta_n})^{-1}[\overline{\mathbf{R}}] = & \mathbf{R} & \hookrightarrow & \mathbf{R}_1 \times \cdots \times \mathbf{R}_n & \\ & \big\downarrow^{\nu_\theta} & & \big\downarrow^{\nu_{\theta_1}} \qquad \big\downarrow^{\nu_{\theta_n}} & \\ \mathbf{R}/\theta|_{\mathbf{R}} = & \overline{\mathbf{R}} & \hookrightarrow & \overline{\mathbf{R}}_1 \times \cdots \times \overline{\mathbf{R}}_n & \cong (\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)/\theta \end{array}$$

Let $\mathcal{V}$ be a variety with a d-cube term.
Let $\mathbf{R} \leq_{\mathrm{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$.

- Assume $\mathbf{R}$ is a *critical subalgebra* of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$, that is,
  - $\mathbf{R}$ is completely $\cap$-irreducible in $\mathrm{Sub}(\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)$, and
  - $\mathbf{R}$ is *directly indecomposable*, i.e., $[n]$ has no partition $\{I, J\}$ such that $\mathbf{R}$ and $\mathbf{R}|_I \times \mathbf{R}|_J$ differ only by a permutation of coordinates.
- Let $\theta = \theta_1 \times \cdots \times \theta_n$ ($\theta_i \in \mathrm{Con}(\mathbf{R}_i)$) be the largest product congruence of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ such that $\mathbf{R}$ is *θ-saturated*, i.e.,

$$\mathbf{R}[\theta] := (\nu_{\theta_1} \times \ldots \times \nu_{\theta_n})^{-1}[\overline{\mathbf{R}}] = \mathbf{R}$$

$$\begin{array}{ccccccc} \mathbf{R} & \hookrightarrow & \mathbf{R}_1 & \times \cdots \times & \mathbf{R}_n & & \\ \downarrow{\scriptstyle \nu_\theta} & & \downarrow{\scriptstyle \nu_{\theta_1}} & & \downarrow{\scriptstyle \nu_{\theta_n}} & & \\ \mathbf{R}/\theta|_{\mathbf{R}} = \overline{\mathbf{R}} & \hookrightarrow & \overline{\mathbf{R}}_1 & \times \cdots \times & \overline{\mathbf{R}}_n & \cong & (\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)/\theta \end{array}$$

Critical Algebras in Varieties with a Cube Term: Reduction

Let $\mathcal{V}$ be a variety with a d-cube term.
Let $\mathbf{R} \leq_{\mathrm{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$.

- Assume $\mathbf{R}$ is a *critical subalgebra* of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$, that is,
  - $\mathbf{R}$ is completely $\cap$-irreducible in $\mathrm{Sub}(\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)$, and
  - $\mathbf{R}$ is *directly indecomposable*, i.e., $[n]$ has no partition $\{I, J\}$ such that $\mathbf{R}$ and $\mathbf{R}|_I \times \mathbf{R}|_J$ differ only by a permutation of coordinates.
- Let $\theta = \theta_1 \times \cdots \times \theta_n$ ($\theta_i \in \mathrm{Con}(\mathbf{R}_i)$) be the largest product congruence of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ such that $\mathbf{R}$ is *θ-saturated*, i.e.,

$$
\begin{array}{rcccl}
\mathbf{R}[\theta] := (\nu_{\theta_1} \times \ldots \times \nu_{\theta_n})^{-1}[\overline{\mathbf{R}}] = & \mathbf{R} & \hookrightarrow & \mathbf{R}_1 \times \cdots \times \mathbf{R}_n & \\
 & \big\downarrow{\scriptstyle \nu_\theta} & & \big\downarrow{\scriptstyle \nu_{\theta_1}} \qquad\quad \big\downarrow{\scriptstyle \nu_{\theta_n}} & \\
\mathbf{R}/\theta|_{\mathbf{R}} = & \overline{\mathbf{R}} & \hookrightarrow & \overline{\mathbf{R}}_1 \times \cdots \times \overline{\mathbf{R}}_n & \cong (\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)/\theta
\end{array}
$$

- **Fact.** $a\, \theta_1\, b$ iff $a\mathbf{u}, b\mathbf{u} \in \mathbf{R}$ for some $\mathbf{u} \in \mathbf{R}_2 \times \cdots \times \mathbf{R}_n$.

Let $\mathcal{V}$ be a variety with a d-cube term.
Let $\mathbf{R} \leq_{\mathrm{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$.

- Assume $\mathbf{R}$ is a *critical subalgebra* of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$, that is,
  - $\mathbf{R}$ is completely $\cap$-irreducible in $\mathrm{Sub}(\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)$, and
  - $\mathbf{R}$ is *directly indecomposable*, i.e., $[n]$ has no partition $\{I, J\}$ such that $\mathbf{R}$ and $\mathbf{R}|_I \times \mathbf{R}|_J$ differ only by a permutation of coordinates.
- Let $\theta = \theta_1 \times \cdots \times \theta_n$ ($\theta_i \in \mathrm{Con}(\mathbf{R}_i)$) be the largest product congruence of $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ such that $\mathbf{R}$ is *θ-saturated*, i.e.,

$$
\begin{array}{rcccl}
\mathbf{R}[\theta] := (\nu_{\theta_1} \times \ldots \times \nu_{\theta_n})^{-1}[\overline{\mathbf{R}}] = \mathbf{R} & \hookrightarrow & \mathbf{R}_1 \times \cdots \times \mathbf{R}_n & & \\
\downarrow \nu_\theta & & \downarrow \nu_{\theta_1} \qquad \downarrow \nu_{\theta_n} & & \\
\mathbf{R}/\theta|_{\mathbf{R}} = \overline{\mathbf{R}} & \hookrightarrow & \overline{\mathbf{R}}_1 \times \cdots \times \overline{\mathbf{R}}_n & \cong & (\mathbf{R}_1 \times \cdots \times \mathbf{R}_n)/\theta
\end{array}
$$

- **Fact.** $a\,\theta_1\,b$ iff $a\mathbf{u}, b\mathbf{u} \in \mathbf{R}$ for some $\mathbf{u} \in \mathbf{R}_2 \times \cdots \times \mathbf{R}_n$.

$\overline{\mathbf{R}}$ is *the reduced representation* of $\mathbf{R}$.

Critical Algebras in Varieties with a Cube Term: Structure

Structure Theorem (Kearnes–Sz, 2012)

Let $\mathcal{V}$ be a variety with a d-cube term.

Critical Algebras in Varieties with a Cube Term: Structure

Structure Theorem (Kearnes–Sz, 2012)

Let $\mathcal{V}$ be a variety with a d-cube term.
If $\overline{\mathbf{R}}$ is the reduced representation of a critical subalgebra
$\mathbf{R} \leq_{\mathrm{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ *with* $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$ *and* $n \geq d$*, then*

Critical Algebras in Varieties with a Cube Term: Structure

Structure Theorem (Kearnes–Sz, 2012)

Let $\mathcal{V}$ be a variety with a d-cube term.
If $\overline{\mathbf{R}}$ is the reduced representation of a critical subalgebra $\mathbf{R} \leq_{\mathrm{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$ and $n \geq d$, then

- $\overline{\mathbf{R}}_1, \ldots, \overline{\mathbf{R}}_n$ *are similar SIs;*

Critical Algebras in Varieties with a Cube Term: Structure

Structure Theorem (Kearnes–Sz, 2012)

Let $\mathcal{V}$ be a variety with a d-cube term.
If $\overline{\mathbf{R}}$ is the reduced representation of a critical subalgebra $\mathbf{R} \leq_{\mathrm{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$ and $n \geq d$, then

- $\overline{\mathbf{R}}_1, \ldots, \overline{\mathbf{R}}_n$ *are similar SIs;*
- *if $n \geq 3$, then each $\overline{\mathbf{R}}_i$ has abelian monolith μ_i $(i \in [n])$; and*

Structure Theorem (Kearnes–Sz, 2012)

Let $\mathcal{V}$ be a variety with a d-cube term.
If $\overline{\mathbf{R}}$ is the reduced representation of a critical subalgebra $\mathbf{R} \leq_{\mathrm{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$ and $n \geq d$, then

- *$\overline{\mathbf{R}}_1, \ldots, \overline{\mathbf{R}}_n$ are similar SIs;*
- *if $n \geq 3$, then each $\overline{\mathbf{R}}_i$ has abelian monolith μ_i $(i \in [n])$; and*
- *for the centralizers $\rho_\ell := (0 : \mu_\ell)$ of the monoliths μ_ℓ $(\ell \in [n])$, the image $\overline{\mathbf{R}}|_{ij}/(\rho_i \times \rho_j)$ of the composite map*

$$\overline{\mathbf{R}} \stackrel{\mathrm{pr}_{ij}}{\to} \overline{\mathbf{R}}_i \times \overline{\mathbf{R}}_j \twoheadrightarrow \overline{\mathbf{R}}_i/\rho_i \times \overline{\mathbf{R}}_j/\rho_j.$$

Critical Algebras in Varieties with a Cube Term: Structure

Structure Theorem (Kearnes–Sz, 2012)

Let $\mathcal{V}$ be a variety with a d-cube term.
If $\overline{\mathbf{R}}$ is the reduced representation of a critical subalgebra $\mathbf{R} \leq_{\mathrm{sd}} \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ with $\mathbf{R}_1, \ldots, \mathbf{R}_n \in \mathcal{V}$ and $n \geq d$, then

- $\overline{\mathbf{R}}_1, \ldots, \overline{\mathbf{R}}_n$ *are similar SIs;*
- *if $n \geq 3$, then each $\overline{\mathbf{R}}_i$ has abelian monolith μ_i $(i \in [n])$; and*
- *for the centralizers $\rho_\ell := (0 : \mu_\ell)$ of the monoliths μ_ℓ $(\ell \in [n])$, the image $\overline{\mathbf{R}}|_{ij}/(\rho_i \times \rho_j)$ of the composite map*

$$\overline{\mathbf{R}} \stackrel{\mathrm{pr}_{ij}}{\to} \overline{\mathbf{R}}_i \times \overline{\mathbf{R}}_j \twoheadrightarrow \overline{\mathbf{R}}_i/\rho_i \times \overline{\mathbf{R}}_j/\rho_j.$$

is the graph of an isomorphism $\overline{\mathbf{R}}_i/\rho_i \to \overline{\mathbf{R}}_j/\rho_j$ for any $i, j \in [n]$.

Applying the Structure Theorem to SMP($\mathcal{K}$): Prelims

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 $c \in \mathbf{B}$?

Applying the Structure Theorem to SMP($\mathcal{K}$): Prelims

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 $c \in \mathbf{B}$?

Assume $\mathcal{V}$ has a d-cube term, and $n \geq d$.

Applying the Structure Theorem to SMP($\mathcal{K}$): Prelims

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 $c \in \mathbf{B}$?

Assume $\mathcal{V}$ has a d-cube term, and $n \geq d$.

Obvious necessary condition for $c \in \mathbf{B}$:

(†) $c|_I \in \mathbf{B}|_I = \langle b_1|_I, \ldots, b_k|_I \rangle$ *for all* $I \in \binom{[n]}{d}$.

Applying the Structure Theorem to SMP($\mathcal{K}$): Prelims

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 $c \in \mathbf{B}$?

Assume $\mathcal{V}$ has a d-cube term, and $n \geq d$.

Obvious necessary condition for $c \in \mathbf{B}$:

(†) $c|_I \in \mathbf{B}|_I = \langle b_1|_I, \ldots, b_k|_I \rangle$ *for all* $I \in \binom{[n]}{d}$.
[Can be checked in polynomial time.]

Applying the Structure Theorem to SMP($\mathcal{K}$): Prelims

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 $c \in \mathbf{B}$?

Assume $\mathcal{V}$ has a d-cube term, and $n \geq d$.

Obvious necessary condition for $c \in \mathbf{B}$:

(†) $c|_I \in \mathbf{B}|_I = \langle b_1|_I, \ldots, b_k|_I \rangle$ *for all* $I \in \binom{[n]}{d}$.
[Can be checked in polynomial time.]

Goal: To strengthen this to a necessary and sufficient condition.

Applying the Structure Theorem to SMP($\mathcal{K}$): Prelims

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 $c \in \mathbf{B}$?

Assume $\mathcal{V}$ has a d-cube term, and $n \geq d$.

Obvious necessary condition for $c \in \mathbf{B}$:

(†) $c|_I \in \mathbf{B}|_I = \langle b_1|_I, \ldots, b_k|_I \rangle$ *for all* $I \in \binom{[n]}{d}$.
[Can be checked in polynomial time.]

Goal: To strengthen this to a necessary and sufficient condition.

Will assume (†) from now on.

Applying the Structure Theorem to SMP($\mathcal{K}$): SIs

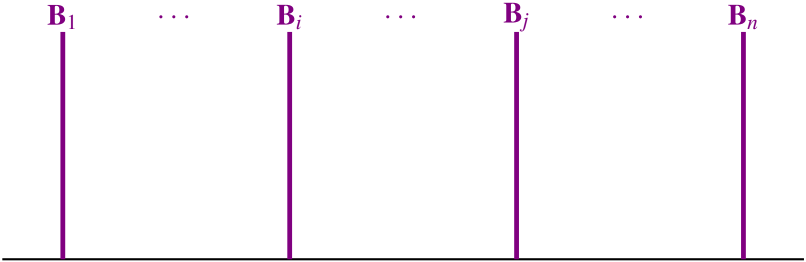
Recall: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ ($\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$)

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

Applying the Structure Theorem to SMP($\mathcal{K}$): SIs

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

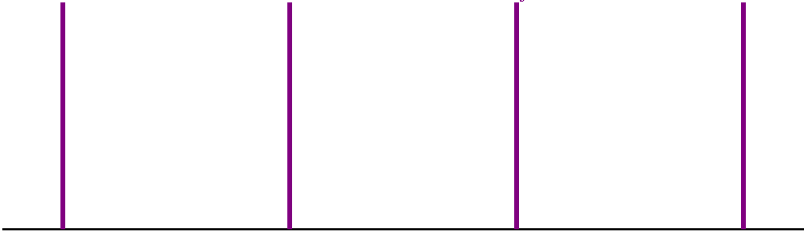
$\mathbf{B} := \langle b_1, \dots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ $(\mathbf{B}_i \leq \mathbf{A}_i)$, c satisfies $(\dagger)$



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

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

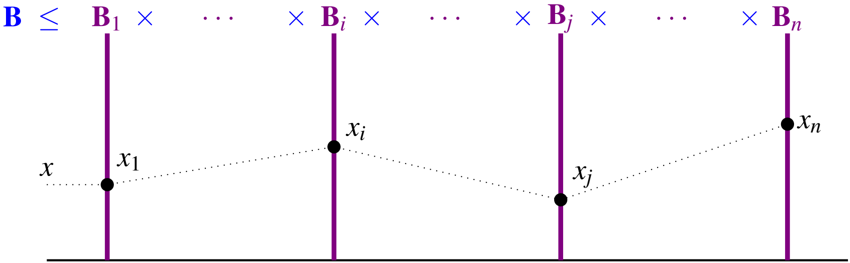
$\mathbf{B} \leq \mathbf{B}_1 \times \cdots \times \mathbf{B}_i \times \cdots \times \mathbf{B}_j \times \cdots \times \mathbf{B}_n$



Applying the Structure Theorem to SMP($\mathcal{K}$): SIs

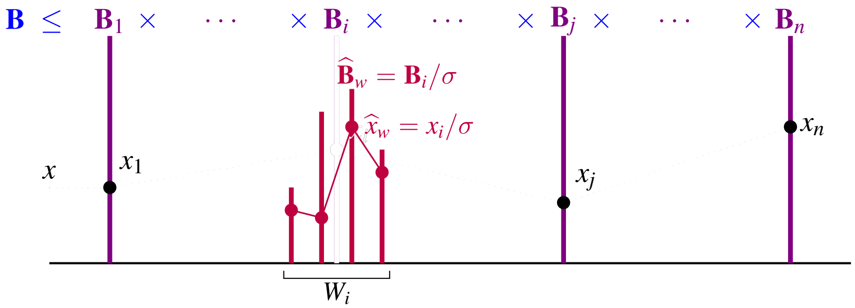
Recall: $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ ($\mathbf{A}_1, \ldots, \mathbf{A}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$)

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



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

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

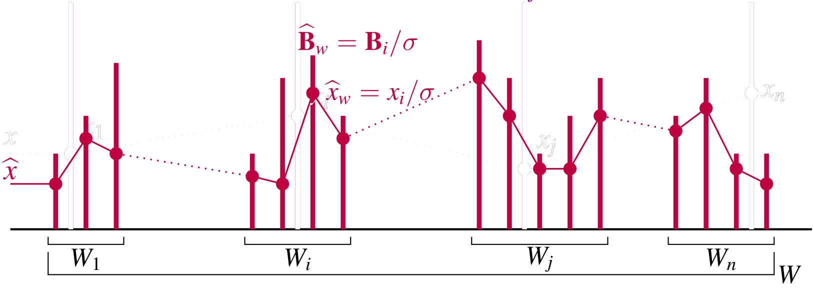


$$\mathbf{B}_i \hookrightarrow \prod_{\sigma \in \mathrm{Con}_{\wedge\text{-irr}}(\mathbf{B}_i)} \underbrace{\mathbf{B}_i/\sigma}_{\widehat{\mathbf{B}}_w}, \quad x_i \mapsto \big(\underbrace{x_i/\sigma}_{\widehat{x}_w}\big)_\sigma \qquad (w=(i,\sigma))$$

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

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

$$\mathbf{B} \leq \mathbf{B}_1 \times \cdots \times \mathbf{B}_i \times \cdots \times \mathbf{B}_j \times \cdots \times \mathbf{B}_n$$



$$\mathbf{B}_i \hookrightarrow \prod_{\sigma \in \mathrm{Con}_{\wedge\text{-irr}}(\mathbf{B}_i)} \underbrace{\mathbf{B}_i/\sigma}_{\widehat{\mathbf{B}}_w}, \quad x_i \mapsto \big(\underbrace{x_i/\sigma}_{\widehat{x}_w}\big)_\sigma \qquad (w=(i,\sigma))$$

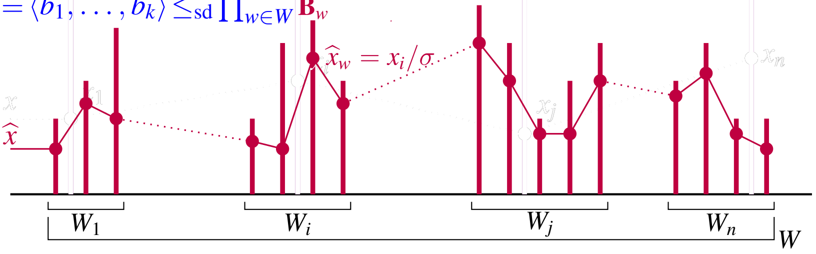
Applying the Structure Theorem to SMP($\mathcal{K}$): SIs

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

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

$\mathbf{B} \leq \mathbf{B}_1 \times \cdots \times \mathbf{B}_i \times \cdots \times \mathbf{B}_j \times \cdots \times \mathbf{B}_n$

$\widehat{\mathbf{B}} = \langle \widehat{b}_1, \dots, \widehat{b}_k \rangle \leq_{\mathrm{sd}} \prod_{w \in W} \widehat{\mathbf{B}}_w$



$$\mathbf{B}_i \hookrightarrow \prod_{\sigma \in \mathrm{Con}_{\wedge\text{-irr}}(\mathbf{B}_i)} \underbrace{\mathbf{B}_i/\sigma}_{\widehat{\mathbf{B}}_w}, \quad x_i \mapsto (\underbrace{x_i/\sigma}_{\widehat{x}_w})_\sigma \qquad (w=(i,\sigma))$$

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

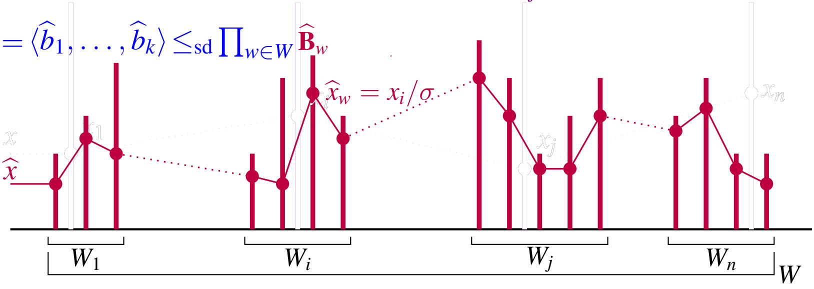
$\mathbf{B} := \langle b_1, \ldots, b_k \rangle \leq_{\mathrm{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ $(\mathbf{B}_i \leq \mathbf{A}_i)$, c satisfies $(\dagger)$

$\boxed{c \in \mathbf{B} \text{ iff } \widehat{c} \in \widehat{\mathbf{B}}}$

$c \in \mathbf{B} \leq \mathbf{B}_1 \times \cdots \times \mathbf{B}_i \times \cdots \times \mathbf{B}_j \times \cdots \times \mathbf{B}_n$

iff

$\widehat{c} \in \widehat{\mathbf{B}} = \langle \widehat{b}_1, \ldots, \widehat{b}_k \rangle \leq_{\mathrm{sd}} \prod_{w \in W} \widehat{\mathbf{B}}_w$



$$\mathbf{B}_i \hookrightarrow \prod_{\sigma \in \mathrm{Con}_{\wedge\text{-irr}}(\mathbf{B}_i)} \underbrace{\mathbf{B}_i/\sigma}_{\widehat{\mathbf{B}}_w}, \quad x_i \mapsto (\underbrace{x_i/\sigma}_{\widehat{x}_w})_\sigma \quad (w=(i,\sigma))$$

Applying the Structure Theorem to SMP($\mathcal{K}$): A Partition

Have: $\widehat{b}_1, \ldots, \widehat{b}_k, \widehat{c} \in \prod_{w \in W} \widehat{\mathbf{B}}_w$ ($\widehat{\mathbf{B}}_w \in \mathbb{HS}\mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$)

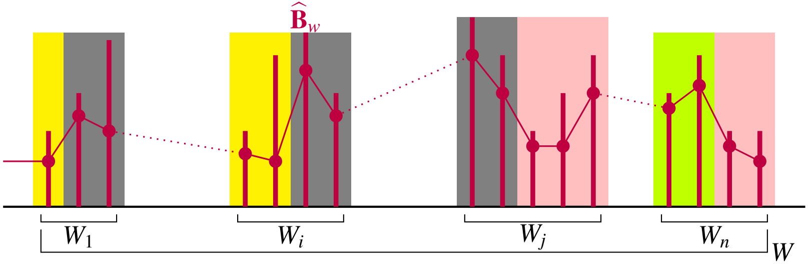
$\widehat{\mathbf{B}} = \langle \widehat{b}_1, \ldots, \widehat{b}_k \rangle \leq_{\text{sd}} \prod_{w \in W} \widehat{\mathbf{B}}_w$ (each $\widehat{\mathbf{B}}_w$ SI with monolith μ_w)

Question: Is $\widehat{c} \in \widehat{B}$? (Assuming c satisfies $(\dagger)$.)

Applying the Structure Theorem to SMP($\mathcal{K}$): A Partition

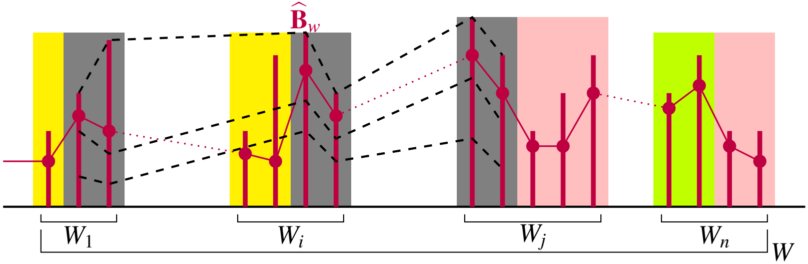
Have: $\widehat{b}_1, \ldots, \widehat{b}_k, \widehat{c} \in \prod_{w\in W} \widehat{\mathbf{B}}_w$ ($\widehat{\mathbf{B}}_w \in \mathbb{HS}\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$)
$\widehat{\mathbf{B}} = \langle \widehat{b}_1, \ldots, \widehat{b}_k \rangle \leq_{\mathrm{sd}} \prod_{w\in W} \widehat{\mathbf{B}}_w$ (each $\widehat{\mathbf{B}}_w$ SI with monolith μ_w)
Question: Is $\widehat{c} \in \widehat{B}$? (Assuming c satisfies $(\dagger)$.)

Easy Fact. *The following relation $\sim$ on W is an equivalence relation: $v \sim w$ iff $v = w$ or $\widehat{\mathbf{B}}_v$, $\widehat{\mathbf{B}}_w$ are similar SIs with abelian monoliths μ_v, μ_w such that*



Have: $\widehat{b}_1, \ldots, \widehat{b}_k, \widehat{c} \in \prod_{w\in W} \widehat{\mathbf{B}}_w$ ($\widehat{\mathbf{B}}_w \in \mathbb{HS}\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$)
$\widehat{\mathbf{B}} = \langle \widehat{b}_1, \ldots, \widehat{b}_k \rangle \leq_{\mathrm{sd}} \prod_{w\in W} \widehat{\mathbf{B}}_w$ (each $\widehat{\mathbf{B}}_w$ SI with monolith μ_w)
Question: Is $\widehat{c} \in \widehat{B}$? (Assuming c satisfies (†).)

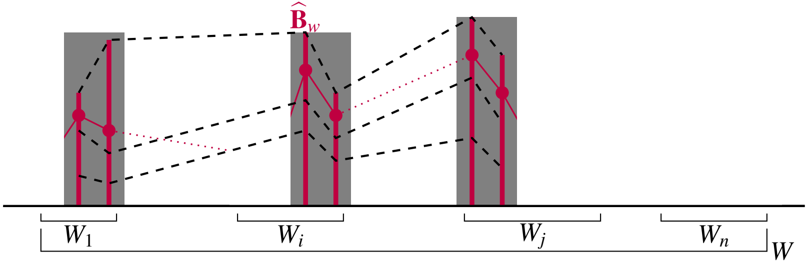
Easy Fact. *The following relation $\sim$ on W is an equivalence relation: $v \sim w$ iff $v = w$ or $\widehat{\mathbf{B}}_v$, $\widehat{\mathbf{B}}_w$ are similar SIs with abelian monoliths μ_v, μ_w such that for the centralizers $\rho_v = (0 : \mu_v)$, $\rho_w = (0 : \mu_w)$, $\widehat{\mathbf{B}}|_{v,w}/(\rho_v \times \rho_w)$ is the graph of an isomorphism $\widehat{\mathbf{B}}_v/\rho_v \to \widehat{\mathbf{B}}_w/\rho_w$.*



Applying the Structure Theorem to SMP($\mathcal{K}$): A Partition

Have: $\widehat{b}_1, \ldots, \widehat{b}_k, \widehat{c} \in \prod_{w\in W} \widehat{\mathbf{B}}_w$ ($\widehat{\mathbf{B}}_w \in \mathbb{HS}\mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$)
$\widehat{\mathbf{B}} = \langle \widehat{b}_1, \ldots, \widehat{b}_k \rangle \leq_{\text{sd}} \prod_{w\in W} \widehat{\mathbf{B}}_w$ (each $\widehat{\mathbf{B}}_w$ SI with monolith μ_w)
Question: Is $\widehat{c} \in \widehat{B}$? (Assuming c satisfies (†).)

Easy Fact. *The following relation $\sim$ on W is an equivalence relation: $v \sim w$ iff $v = w$ or $\widehat{\mathbf{B}}_v$, $\widehat{\mathbf{B}}_w$ are similar SIs with abelian monoliths μ_v, μ_w such that for the centralizers $\rho_v = (0 : \mu_v)$, $\rho_w = (0 : \mu_w)$, $\widehat{\mathbf{B}}|_{v,w}/(\rho_v \times \rho_w)$ is the graph of an isomorphism $\widehat{\mathbf{B}}_v/\rho_v \to \widehat{\mathbf{B}}_w/\rho_w$.*



Applying the Structure Theorem to $\mathrm{SMP}(\mathcal{K})$: A Criterion

Theorem

Let $\mathcal{V}$ be a variety with a d-cube term, and let $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ be an input for $\mathrm{SMP}(\mathcal{K})$ with $n \geq d$ for some finite $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$.

Applying the Structure Theorem to $\mathrm{SMP}(\mathcal{K})$: A Criterion

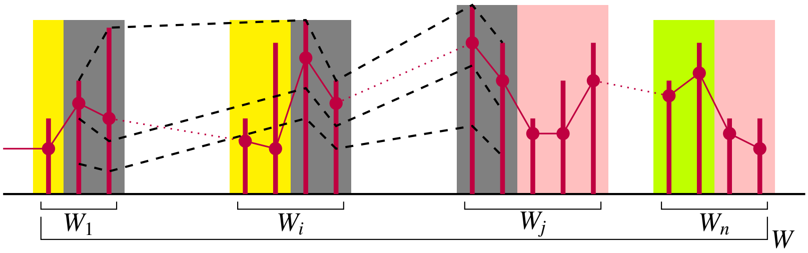
Theorem

Let $\mathcal{V}$ be a variety with a d-cube term, and let $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ be an input for $\mathrm{SMP}(\mathcal{K})$ with $n \geq d$ for some finite $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$.
Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle$,

Applying the Structure Theorem to $\mathrm{SMP}(\mathcal{K})$: A Criterion

Theorem

Let $\mathcal{V}$ be a variety with a d-cube term, and let $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ be an input for $\mathrm{SMP}(\mathcal{K})$ with $n \geq d$ for some finite $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$.
Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle$, and let W, $\widehat{\mathbf{B}}_w$ $(w \in W)$, $\widehat{\mathbf{B}}$, and $\sim$ be as defined above.

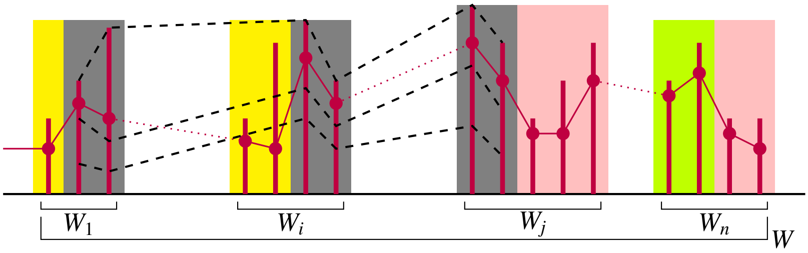


Applying the Structure Theorem to SMP($\mathcal{K}$): A Criterion

Theorem

Let $\mathcal{V}$ be a variety with a d-cube term, and let $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ be an input for SMP($\mathcal{K}$) *with $n \geq d$ for some finite $\mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$.*
Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle$, and let W, $\widehat{\mathbf{B}}_w$ $(w \in W)$, $\widehat{\mathbf{B}}$, and $\sim$ be as defined above.
Then $c \in \mathbf{B}$ holds of and only if

(†) $c|_I \in \mathbf{B}|_I$ *for all* $I \in \binom{[n]}{d}$, *and*

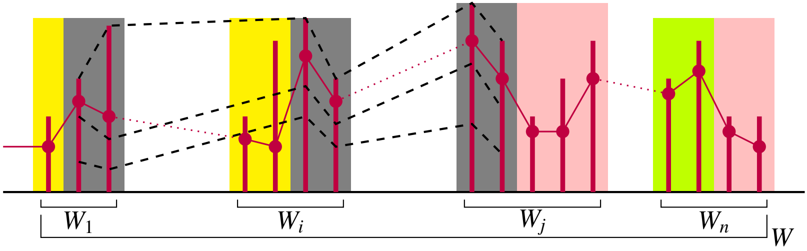


Theorem

Let $\mathcal{V}$ be a variety with a d-cube term, and let $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ be an input for SMP($\mathcal{K}$) *with $n \geq d$ for some finite $\mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$.*
Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle$, and let W, $\widehat{\mathbf{B}}_w$ $(w \in W)$, $\widehat{\mathbf{B}}$, and $\sim$ be as defined above.
Then $c \in \mathbf{B}$ holds of and only if

(†) $c|_I \in \mathbf{B}|_I$ *for all* $I \in \binom{[n]}{d}$, *and*

(‡) $\widehat{c}|_U \in \widehat{\mathbf{B}}|_U$ *for all blocks* U $(\subseteq W)$ *of* $\sim$ *of size* $|U| \geq \max\{d, 3\}$.

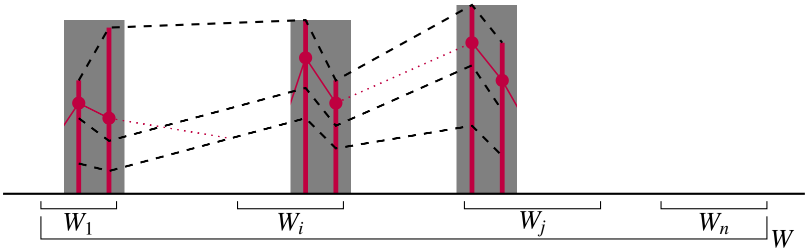


Theorem

Let $\mathcal{V}$ be a variety with a d-cube term, and let $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ be an input for SMP($\mathcal{K}$) *with $n \geq d$ for some finite $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$.*
Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle$, and let W, $\widehat{\mathbf{B}}_w$ $(w \in W)$, $\widehat{\mathbf{B}}$, and $\sim$ be as defined above.
Then $c \in \mathbf{B}$ holds of and only if

($\dagger$) $c|_I \in \mathbf{B}|_I$ *for all* $I \in \binom{[n]}{d}$, *and*

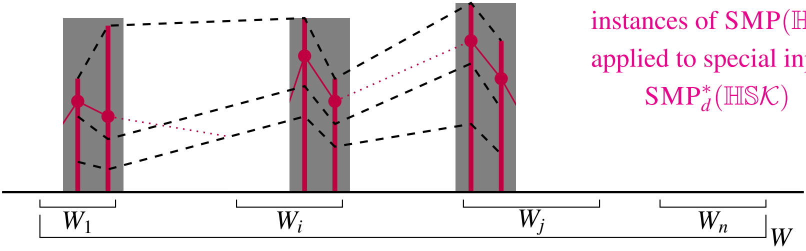
($\ddagger$) $\widehat{c}|_U \in \widehat{\mathbf{B}}|_U$ *for all blocks* U $(\subseteq W)$ *of* $\sim$ *of size* $|U| \geq \max\{d, 3\}$.



Theorem

Let $\mathcal{V}$ be a variety with a d-cube term, and let $b_1, \ldots, b_k, c \in \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ be an input for $\mathrm{SMP}(\mathcal{K})$ with $n \geq d$ for some finite $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$.
Let $\mathbf{B} := \langle b_1, \ldots, b_k \rangle$, and let W, $\widehat{\mathbf{B}}_w$ $(w \in W)$, $\widehat{\mathbf{B}}$, and $\sim$ be as defined above.
Then $c \in \mathbf{B}$ holds of and only if

- (†) $c|_I \in \mathbf{B}|_I$ *for all* $I \in \binom{[n]}{d}$, *and*
- (‡) $\widehat{c}|_U \in \widehat{\mathbf{B}}|_U$ *for all blocks* U $(\subseteq W)$ *of* $\sim$ *of size* $|U| \geq \max\{d, 3\}$.



instances of $\mathrm{SMP}(\mathbb{HS}\mathcal{K})$ applied to special inputs: $\mathrm{SMP}^*_d(\mathbb{HS}\mathcal{K})$

Applying the Structure Theorem to $\mathrm{SMP}(\mathcal{K})$: A Corollary

Corollary

Let $\mathcal{V}$ be a variety with a d-cube term.
For every finite $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$,

$$\mathrm{SMP}(\mathcal{K}) \quad \overset{\text{poly time}}{\Longleftrightarrow} \quad \mathrm{SMP}_d^*(\mathbb{H}\mathbb{S}\mathcal{K}).$$

The RS Case: Prelim

Assume:

(∗) $\mathcal{V}$ is a RS variety with a d-cube term.

The RS Case: Prelim

Assume:

($*$) $\mathcal{V}$ is a RS variety with a d-cube term.

Recall: Our goal is to prove

Main Theorem. $(*) \Rightarrow \mathrm{SMP}(\mathcal{K}) \in \mathsf{P}$ *for all finite* $\mathcal{K} \subseteq \mathcal{V}_{\text{fin}}$.

Assume:

$(*)$ $\mathcal{V}$ is a RS variety with a d-cube term.

Recall: Our goal is to prove

Main Theorem. $(*) \;\Rightarrow\; \mathrm{SMP}(\mathcal{K}) \in \mathsf{P}$ *for all finite* $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$.

Enough to show:

Claim. $(*) \;\Rightarrow\; \mathrm{SMP}_d^*(\mathcal{K}) \in \mathsf{P}$ *for all finite* $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$.

The RS Case: Prelim

Assume:

$(*)$ $\mathcal{V}$ is a RS variety with a d-cube term.

Recall: Our goal is to prove

Main Theorem. $(*) \;\Rightarrow\; \mathrm{SMP}(\mathcal{K}) \in \mathsf{P}$ *for all finite* $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$.

Enough to show:

Claim. $(*) \;\Rightarrow\; \mathrm{SMP}^*_d(\mathcal{K}) \in \mathsf{P}$ *for all finite* $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$.

Important Facts.

- $\mathcal{V}$ has a cube term $\Rightarrow$ $\mathcal{V}$ CM.
  (BIMMVW, 2010)

The RS Case: Prelim

Assume:

$(*)$ $\mathcal{V}$ is a RS variety with a d-cube term.

Recall: Our goal is to prove

Main Theorem. $(*) \;\Rightarrow\; \mathrm{SMP}(\mathcal{K}) \in \mathsf{P}$ *for all finite* $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$.

Enough to show:

Claim. $(*) \;\Rightarrow\; \mathrm{SMP}_d^*(\mathcal{K}) \in \mathsf{P}$ *for all finite* $\mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$.

Important Facts.

- $\mathcal{V}$ has a cube term $\;\Rightarrow\;$ $\mathcal{V}$ CM.
  (BIMMVW, 2010)
- $\mathcal{V}$ CM & RS $\;\Rightarrow\;$ for every SI $\mathbf{S} \in \mathcal{V}$ with abelian monolith μ,
  the centralizer $\rho = (0 : \mu)$ is abelian.
  (Freese, McKenzie, 1981)

The RS Case: Idea of Proof

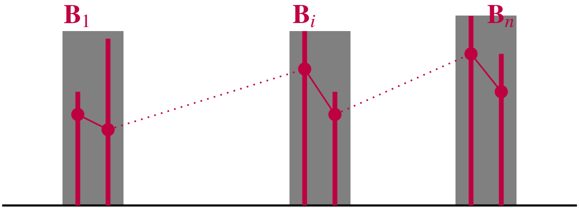
INPUT: $b_1, \ldots, b_k, c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ ($\mathbf{B}_1, \ldots, \mathbf{B}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}},\ n \geq d, 3$) s.t.

- $\mathbf{B} := \langle b_1, \ldots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ and $c|_I \in \mathbf{B}|_I$ for all $I \in \binom{[n]}{d}$

The RS Case: Idea of Proof

INPUT: $b_1, \dots, b_k, c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ $(\mathbf{B}_1, \dots, \mathbf{B}_n \in \mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}},\ n \geq d, 3)$ s.t.

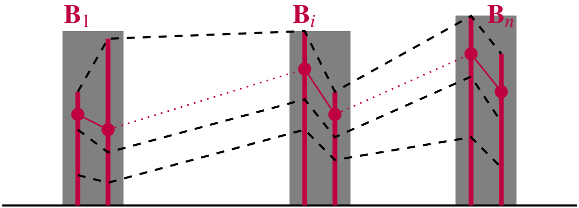
- $\mathbf{B} := \langle b_1, \dots, b_k \rangle \leq_{\mathrm{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ and $c|_I \in \mathbf{B}|_I$ for all $I \in \binom{[n]}{d}$
- $\mathbf{B}_i$s are similar SIs with abelian monoliths μ_i; let $\rho_i := (0 : \mu_i)$



The RS Case: Idea of Proof

INPUT: $b_1, \ldots, b_k, c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ ($\mathbf{B}_1, \ldots, \mathbf{B}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}},\ n \geq d, 3$) s.t.

- $\mathbf{B} := \langle b_1, \ldots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ and $c|_I \in \mathbf{B}|_I$ for all $I \in \binom{[n]}{d}$
- $\mathbf{B}_i$s are similar SIs with abelian monoliths μ_i; let $\rho_i := (0 : \mu_i)$
- $\mathbf{B}|_{ij}/(\rho_i \times \rho_j)$ is the graph of an isomorphism $\mathbf{B}_i/\rho_i \to \mathbf{B}_j/\rho_j$ for all i, j

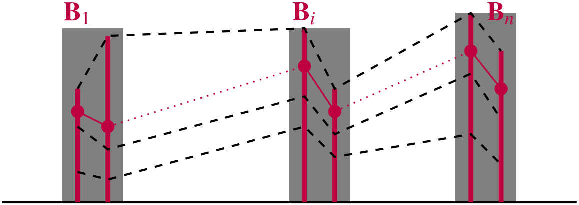


The RS Case: Idea of Proof

INPUT: $b_1, \ldots, b_k, c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ ($\mathbf{B}_1, \ldots, \mathbf{B}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}},\ n \geq d, 3$) s.t.

- $\mathbf{B} := \langle b_1, \ldots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ and $c|_I \in \mathbf{B}|_I$ for all $I \in \binom{[n]}{d}$
- $\mathbf{B}_i$s are similar SIs with abelian monoliths μ_i; let $\rho_i := (0 : \mu_i)$
- $\mathbf{B}|_{ij}/(\rho_i \times \rho_j)$ is the graph of an isomorphism $\mathbf{B}_i/\rho_i \to \mathbf{B}_j/\rho_j$ for all i, j

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

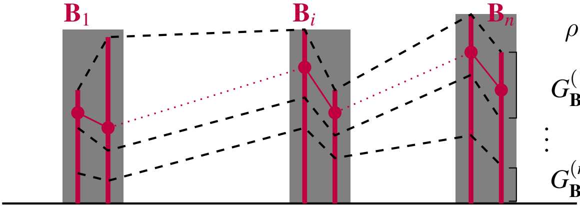


The RS Case: Idea of Proof

INPUT: $b_1, \dots, b_k, c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ ($\mathbf{B}_1, \dots, \mathbf{B}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}},\ n \geq d, 3$) s.t.

- $\mathbf{B} := \langle b_1, \dots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ and $c|_I \in \mathbf{B}|_I$ for all $I \in \binom{[n]}{d}$
- $\mathbf{B}_i$s are similar SIs with abelian monoliths μ_i; let $\rho_i := (0 : \mu_i)$
- $\mathbf{B}|_{ij}/(\rho_i \times \rho_j)$ is the graph of an isomorphism $\mathbf{B}_i/\rho_i \to \mathbf{B}_j/\rho_j$ for all i, j

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



$\rho = \rho_1 \times \cdots \times \rho_n$ classes:

$$G^{(1)}_{\mathbf{B}[\theta]} = G^{(1)}_{\mathbf{B}_1} \times \cdots \times G^{(1)}_{\mathbf{B}_n}$$

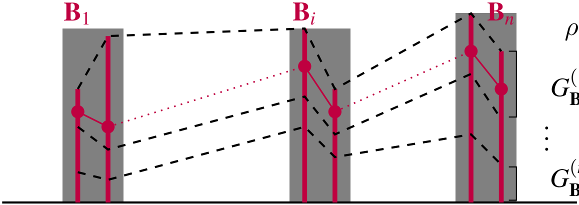
$$\vdots$$

$$G^{(m)}_{\mathbf{B}[\theta]} = G^{(m)}_{\mathbf{B}_1} \times \cdots \times G^{(m)}_{\mathbf{B}_n}$$

INPUT: $b_1, \dots, b_k, c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ ($\mathbf{B}_1, \dots, \mathbf{B}_n \in \mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}},\ n \geq d, 3$) s.t.

- $\mathbf{B} := \langle b_1, \dots, b_k \rangle \leq_{\mathrm{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ and $c|_I \in \mathbf{B}|_I$ for all $I \in \binom{[n]}{d}$
- $\mathbf{B}_i$s are similar SIs with abelian monoliths μ_i; let $\rho_i := (0 : \mu_i)$
- $\mathbf{B}|_{ij}/(\rho_i \times \rho_j)$ is the graph of an isomorphism $\mathbf{B}_i/\rho_i \to \mathbf{B}_j/\rho_j$ for all i, j

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



$\rho = \rho_1 \times \cdots \times \rho_n$ classes:

$$G^{(1)}_{\mathbf{B}[\theta]} = G^{(1)}_{\mathbf{B}_1} \times \cdots \times G^{(1)}_{\mathbf{B}_n}$$

$$\vdots$$

$$G^{(m)}_{\mathbf{B}[\theta]} = G^{(m)}_{\mathbf{B}_1} \times \cdots \times G^{(m)}_{\mathbf{B}_n}$$

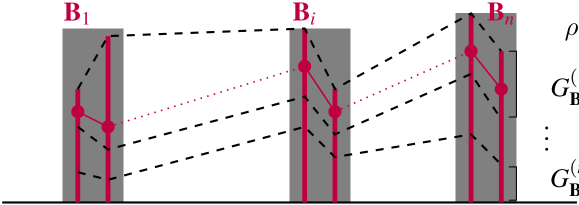
ρ abelian $\Rightarrow$ ► each $G^{(\ell)}_{\mathbf{B}[\theta]}$ is an abelian group (choose zero $o^{(\ell)} \in \mathbf{B}$)

The RS Case: Idea of Proof

INPUT: $b_1, \ldots, b_k, c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ ($\mathbf{B}_1, \ldots, \mathbf{B}_n \in \mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}},\ n \geq d, 3$) s.t.

- $\mathbf{B} := \langle b_1, \ldots, b_k \rangle \leq_{\mathrm{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ and $c|_I \in \mathbf{B}|_I$ for all $I \in \binom{[n]}{d}$
- $\mathbf{B}_i$s are similar SIs with abelian monoliths μ_i; let $\rho_i := (0 : \mu_i)$
- $\mathbf{B}|_{ij}/(\rho_i \times \rho_j)$ is the graph of an isomorphism $\mathbf{B}_i/\rho_i \to \mathbf{B}_j/\rho_j$ for all i, j

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



$\rho = \rho_1 \times \cdots \times \rho_n$ classes:

$$G^{(1)}_{\mathbf{B}[\theta]} = G^{(1)}_{\mathbf{B}_1} \times \cdots \times G^{(1)}_{\mathbf{B}_n}$$

$$\vdots$$

$$G^{(m)}_{\mathbf{B}[\theta]} = G^{(m)}_{\mathbf{B}_1} \times \cdots \times G^{(m)}_{\mathbf{B}_n}$$

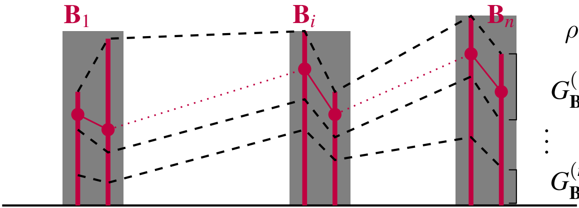
ρ abelian $\Rightarrow$
- ▶ each $G^{(\ell)}_{\mathbf{B}[\theta]}$ is an abelian group (choose zero $o^{(\ell)} \in \mathbf{B}$)
- ▶ operations are (affine) linear between the blocks

The RS Case: Idea of Proof

INPUT: $b_1, \dots, b_k, c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ ($\mathbf{B}_1, \dots, \mathbf{B}_n \in \mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}}$, $n \geq d, 3$) s.t.

- $\mathbf{B} := \langle b_1, \dots, b_k \rangle \leq_{\mathrm{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ and $c|_I \in \mathbf{B}|_I$ for all $I \in \binom{[n]}{d}$
- $\mathbf{B}_i$s are similar SIs with abelian monoliths μ_i; let $\rho_i := (0 : \mu_i)$
- $\mathbf{B}|_{ij}/(\rho_i \times \rho_j)$ is the graph of an isomorphism $\mathbf{B}_i/\rho_i \to \mathbf{B}_j/\rho_j$ for all i, j

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



$\rho = \rho_1 \times \cdots \times \rho_n$ classes:

$$G^{(1)}_{\mathbf{B}[\theta]} = G^{(1)}_{\mathbf{B}_1} \times \cdots \times G^{(1)}_{\mathbf{B}_n}$$

$$\vdots$$

$$G^{(m)}_{\mathbf{B}[\theta]} = G^{(m)}_{\mathbf{B}_1} \times \cdots \times G^{(m)}_{\mathbf{B}_n}$$

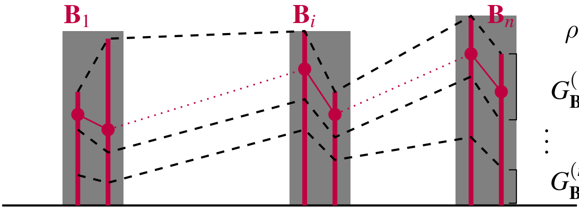
ρ abelian $\Rightarrow$
- each $G^{(\ell)}_{\mathbf{B}[\theta]}$ is an abelian group (choose zero $o^{(\ell)} \in \mathbf{B}$)
- operations are (affine) linear between the blocks
- each $G^{(\ell)}_{\mathbf{B}}$ is a subgroup of $G^{(\ell)}_{\mathbf{B}[\theta]} = G^{(\ell)}_{\mathbf{B}_1} \times \cdots \times G^{(\ell)}_{\mathbf{B}_n}$

The RS Case: Idea of Proof

INPUT: $b_1, \dots, b_k, c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ ($\mathbf{B}_1, \dots, \mathbf{B}_n \in \mathcal{K} \subseteq \mathcal{V}_{\text{fin}},\ n \geq d, 3$) s.t.

- $\mathbf{B} := \langle b_1, \dots, b_k \rangle \leq_{\text{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ and $c|_I \in \mathbf{B}|_I$ for all $I \in \binom{[n]}{d}$
- $\mathbf{B}_i$s are similar SIs with abelian monoliths μ_i; let $\rho_i := (0 : \mu_i)$
- $\mathbf{B}|_{ij}/(\rho_i \times \rho_j)$ is the graph of an isomorphism $\mathbf{B}_i/\rho_i \to \mathbf{B}_j/\rho_j$ for all i, j

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



$\rho = \rho_1 \times \cdots \times \rho_n$ classes:

$$G^{(1)}_{\mathbf{B}[\theta]} = G^{(1)}_{\mathbf{B}_1} \times \cdots \times G^{(1)}_{\mathbf{B}_n}$$

$$\vdots$$

$$G^{(m)}_{\mathbf{B}[\theta]} = G^{(m)}_{\mathbf{B}_1} \times \cdots \times G^{(m)}_{\mathbf{B}_n}$$

ρ abelian $\Rightarrow$
- each $G^{(\ell)}_{\mathbf{B}[\theta]}$ is an abelian group (choose zero $o^{(\ell)} \in \mathbf{B}$)
- operations are (affine) linear between the blocks
- each $G^{(\ell)}_{\mathbf{B}}$ is a subgroup of $G^{(\ell)}_{\mathbf{B}[\theta]} = G^{(\ell)}_{\mathbf{B}_1} \times \cdots \times G^{(\ell)}_{\mathbf{B}_n}$

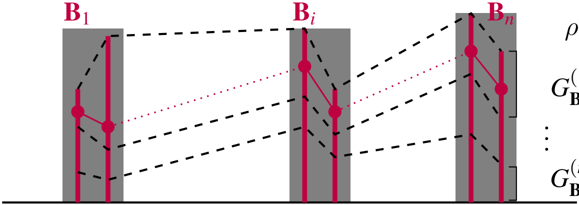
We have $c \in G^{(r)}_{\mathbf{B}[\theta]}$ for some r and $G^{(\ell)}_{\mathbf{B}[\theta]} \cap \mathbf{B} = G^{(\ell)}_{\mathbf{B}}$ for all ℓ

The RS Case: Idea of Proof

INPUT: $b_1, \dots, b_k, c \in \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ ($\mathbf{B}_1, \dots, \mathbf{B}_n \in \mathcal{K} \subseteq \mathcal{V}_{\mathrm{fin}},\ n \geq d, 3$) s.t.

- $\mathbf{B} := \langle b_1, \dots, b_k \rangle \leq_{\mathrm{sd}} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ and $c|_I \in \mathbf{B}|_I$ for all $I \in \binom{[n]}{d}$
- $\mathbf{B}_i$s are similar SIs with abelian monoliths μ_i; let $\rho_i := (0 : \mu_i)$
- $\mathbf{B}|_{ij}/(\rho_i \times \rho_j)$ is the graph of an isomorphism $\mathbf{B}_i/\rho_i \to \mathbf{B}_j/\rho_j$ for all i, j

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



$\rho = \rho_1 \times \cdots \times \rho_n$ classes:

$$G^{(1)}_{\mathbf{B}[\theta]} = G^{(1)}_{\mathbf{B}_1} \times \cdots \times G^{(1)}_{\mathbf{B}_n}$$

$$\vdots$$

$$G^{(m)}_{\mathbf{B}[\theta]} = G^{(m)}_{\mathbf{B}_1} \times \cdots \times G^{(m)}_{\mathbf{B}_n}$$

ρ abelian $\Rightarrow$
- each $G^{(\ell)}_{\mathbf{B}[\theta]}$ is an abelian group (choose zero $o^{(\ell)} \in \mathbf{B}$)
- operations are (affine) linear between the blocks
- each $G^{(\ell)}_{\mathbf{B}}$ is a subgroup of $G^{(\ell)}_{\mathbf{B}[\theta]} = G^{(\ell)}_{\mathbf{B}_1} \times \cdots \times G^{(\ell)}_{\mathbf{B}_n}$

We have $c \in G^{(r)}_{\mathbf{B}[\theta]}$ for some r and $G^{(\ell)}_{\mathbf{B}[\theta]} \cap \mathbf{B} = G^{(\ell)}_{\mathbf{B}}$ for all ℓ

Hence, a modified group algorithm decides $c \in G^{(r)}_{\mathbf{B}}$ ($\Leftrightarrow c \in \mathbf{B}$)