Algebras with polynomially-many homomorphisms

LiBor Barto
William DeMeo
Antoine Mottet

Charles University

Feb 5, 2021 AAA 100

CoCoSym: Symmetry in Computational Complexity

This project has received funding from the European Research Council (ERC) under the European Unions Horizon 2020 research and innovation program (grant agreement No 771 005)

STORY

- we encountered a very natural algebraic question
- we found an answer
- we wonder whether it was studied / known

tell ~~me~~ us
after the talk
!

OUTLINE

- the origin
- the question

+ partial answers, etc.

- the answer

UNIVERSES ARE FINITE

in this talk

THE **ORIGIN**

$\boxed{\text{CSP}}$ Constraint Satisfaction Problem

- CSP over $\mathbb{A}$ ... relational structure

  INPUT: $\mathbb{I}$ of the same signature

  QUESTION: $\exists$ homomorphism $\mathbb{I} \to \mathbb{A}$?

[Schaefer '78]
[Feder, Vardi '98]
[Bulatov, Jeavons, Krokhin '05]
[Bulatov '07] [Zhuk '17]

why not? • CSP over $\mathcal{A}$ ... structure

  INPUT: $\mathcal{I}$ — " —

  QUESTION: — " —

[Feder, Madelaine, Stewart '04]

in particular • CSP over $\underline{\mathbf{A}}$ ... algebra

  INPUT: $\underline{\mathbf{I}}$ of the same signature

  QUESTION: $\exists$ homomorphism $\underline{\mathbf{I}} \to \underline{\mathbf{A}}$?

$\boxed{\text{Fact}}$ $\forall \mathbb{A}$

$\exists \underline{\mathbf{B}}$ with 2 unary op.

$\mathrm{CSP}(\mathbb{A}) \sim \mathrm{CSP}(\underline{\mathbf{B}})$

Turing reduction

FIRST STEPS

- **Fact** [FMS'04] $\mathcal{A}$ contains only unary / constant operations

  $\Rightarrow$ CSP over $\mathcal{A}$ $\sim$ CSP over graph of $\mathcal{A}$

  graph of $f : A^2 \to A$ is $\{(a, b, f(a,b)) ; a, b \in A\}$

- Let's consider $\underline{A}$ with 2-element universes
  - $\uparrow$ unary algebras ✓
  - algebras with an idempotent element ✓

    $e \in A$ such that $\forall f \in \mathrm{Clo}(\underline{A})\ f(e, \dots, e) = e$

  - $\underline{A} = (\{0,1\}; *)$

$*$	0	1
0	1	0
1	0	0

    ✓

    - tried consistency methods

      ...

    - can enforce $\underline{I}$ satisfies identities true in $\underline{A}$
    - adding term operations to $\underline{A}$ does not change complexity
    - $\underline{A}$ is term-equivalent to the 2-element Boolean algebra

TWO

Suppose $\underline{\mathbf{A}} \models s \approx t$. Then there is a polynomial algorithm transforming $\underline{\mathbf{I}}$ to $\underline{\mathbf{I}}'$ so that $(\exists\, \underline{\mathbf{I}} \to \underline{\mathbf{A}}$ iff $\exists\, \underline{\mathbf{I}}' \to \underline{\mathbf{A}})$ & $\underline{\mathbf{I}}' \models s \approx t$

If $\mathrm{Clo}(\underline{\mathbf{A}}) = \mathrm{Clo}(\underline{\mathbf{B}})$ then CSP over $\underline{\mathbf{A}}$ $\sim$ CSP over $\underline{\mathbf{B}}$

$\boxed{\text{A question}}$ How hard is to find the smallest $\alpha \in \mathrm{Con}(\underline{\mathbf{I}})$ such that $\underline{\mathbf{I}}/\alpha \in \mathrm{var}(\underline{\mathbf{A}})$? ($\ldots \in SP(\underline{\mathbf{A}})$?)

not "the"

- $\uparrow$ in P for fixed finitely based $\underline{\mathbf{A}}$ (of finite signature)

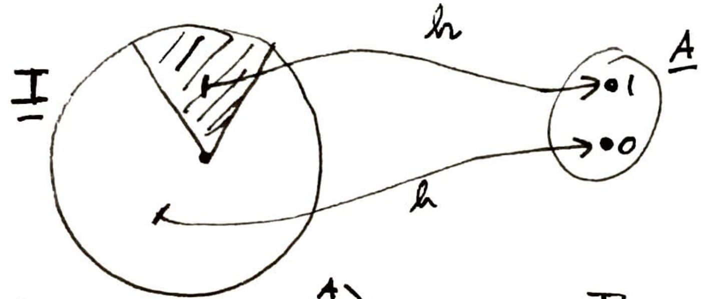
- back to 2-element algebras
- $\boxed{\text{Fact}}$ if not essentially unary, then contains a semilattice, majority, or minority term-operation $\rightsquigarrow$ goal: understand homomorphisms to these

2-ELEMENT ALGEBRAS

every $\mathbf{A}$ that contains such a term operation is ✓

- $\underline{A} = (\{0,1\}; x+y+z)$ term equivalent to 1-dim affine space over $\mathbb{Z}/2\mathbb{Z}$ ✓+
- $\underline{A} = (\{0,1\}; \wedge^{\underline{A}})$, $\underline{I} = (I; \wedge^{\underline{I}})$ WLOG semilattice

  $a \wedge b = \min\{a,b\}$



$\forall h: \underline{I} \to \underline{A}$
$\exists i \in I \quad h(j) = 1$ iff $j \geq i$ ✓+

- $\underline{A} = (\{0,1\}; maj^{\underline{A}})$ $\quad \underline{I} = (I; maj^{\underline{I}})$

  ternary majority

  semilattice!

  if $h(i) = 0$ then h preserves $\begin{cases} s^{\underline{A}}(x,y) := maj^{\underline{A}}(0,x,y) \\ s^{\underline{I}}(x,y) := maj^{\underline{I}}(i,x,y) \end{cases}$ $\rightsquigarrow$ ✓+

$\Rightarrow$ classification of computational complexity for CSPs over 2-element <u>structures</u>

THE **QUESTION**

THE QUESTION: WHAT IS $\mathcal{K}$?

$$\mathcal{K} = \{ \underline{A} : \exists \text{polynomial } p \ \ \forall \underline{I} \text{ of the same signature as } \underline{A} \ \ |\{h : \underline{I} \to \underline{A} : h \text{ homomorphism}\}| < p(|I|) \}$$

(effective variant)

☺ $\mathcal{K}$ is closed under

- S $\underline{B} \in \mathcal{K},\ \underline{A} \leq \underline{B} \Rightarrow \underline{A} \in \mathcal{K}$
- P $\underline{A}, \underline{B} \in \mathcal{K}$ (same sign.) $\Rightarrow \underline{A} \times \underline{B} \in \mathcal{K}$
- E $\underline{B} \in \mathcal{K} \quad \mathrm{Clo}(\underline{B}) \subseteq \mathrm{Clo}(\underline{A}) \Rightarrow \underline{A} \in \mathcal{K}$

not closed under quotients

☹ $\underline{A} \in \mathcal{K} \Leftrightarrow \forall \underline{B} \leq \underline{A} \quad \underline{B} + \text{constants} \in \mathcal{K}$

→ bad news & good news

Examples

- 2-element semilattice $\in \mathcal{K}$
  $\forall$ semilattice $\in \mathcal{K}$
- 2-element majority algebra $\in \mathcal{K}$
- $(\mathbb{Z}_p; x-y+z) \in \mathcal{K}$

($\Rightarrow$ 2-element "non-unary" algebra $\in \mathcal{K}$)

ROCK - PAPER - SCISSORS

$\underline{A} = (\{0,1,2\};\ \cdot^{\underline{A}},\ 0^{\underline{A}}, 1^{\underline{A}}, 2^{\underline{A}})$

$x \cdot^{A} y$ = looser

$0\cdot 1 = 1 \cdot 0 = 0 = 0 \cdot 0$
$1 \cdot 2 = 2 \cdot 1 = 1 = 1 \cdot 1$
$0 \cdot 2 = 2 \cdot 0 = 2 = 2 \cdot 2$

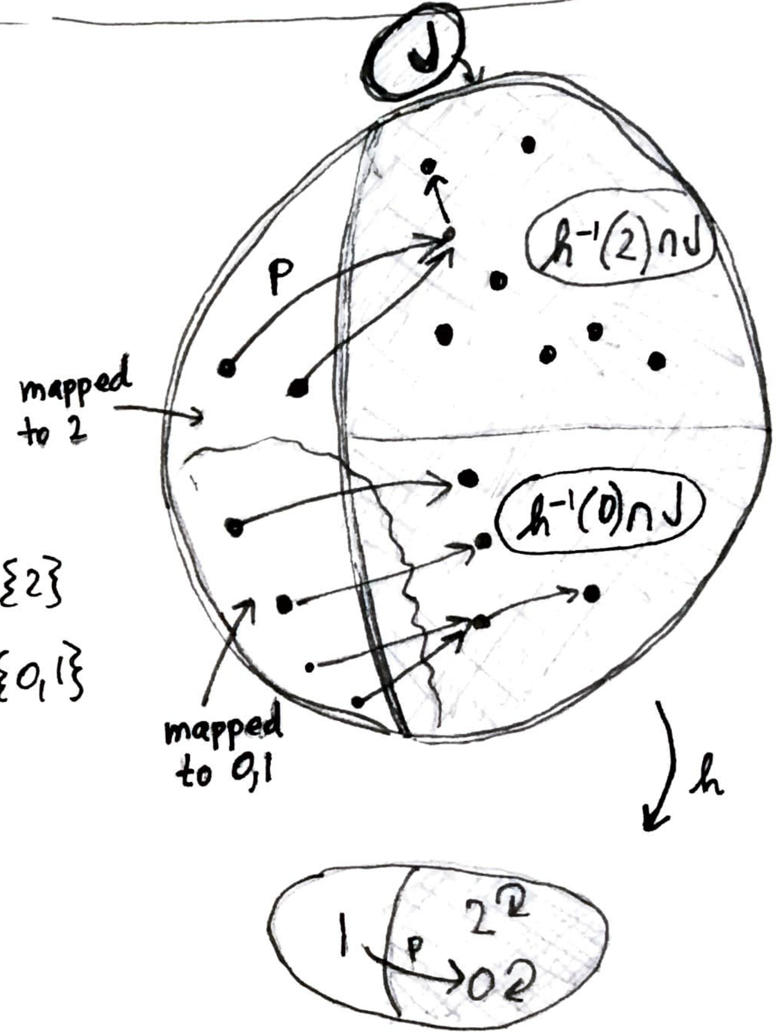
rock 0 $\leq$ 1 paper
$0 \geq 2$ scissors
$2 \geq 1$

- take $\underline{I} = (I;\ \cdot^{\underline{I}}, 0^{\underline{I}}, 1^{\underline{I}}, 2^{\underline{I}})$, $h: \underline{I} \to \underline{A}$
- consider $p(x) = x \cdot 0$

x	0	1	2
$p^{\underline{A}}(x)$	0	0	2

- $J := p^{\underline{I}}(I)$ $\quad h(J) \subseteq \{0,2\}$
- Fix $h_{\restriction J}$, for $j \in J$ $\cdot\ h(j) = 2 \Rightarrow h(p^{-1}(j)) = \{2\}$
  $\cdot\ h(j) = 0 \Rightarrow h(p^{-1}(j)) \subseteq \{0,1\}$

$\rightsquigarrow$ polynomially many $h_{\restriction J}$, for each $h_{\restriction J}$ only polynomially many extensions



images of polynomials, separation, ... $\rightsquigarrow$ Tame Congruence Theory [Hobby, McKenzie '88]

TAYLOR ALGEBRAS IN $\mathcal{K}$

with all constants

Fact $\underline{\mathbf{A}} \in \mathcal{K}$ provided that $\exists \alpha \in \mathrm{Con}(\underline{\mathbf{A}})$ such that

- $\underline{\mathbf{A}}/\alpha \in \mathcal{K}$
- $\forall a \neq b \ (a,b) \in \alpha \ \exists f \in \mathrm{Clo}_1 \underline{\mathbf{A}}$ such that $f(a) \neq f(b)$ and $\underline{\mathbf{A}} \restriction f(a/\alpha) \in \mathcal{K}$

Fact $\underline{\mathbf{A}}$ with constants is in $\mathcal{K}$ <u>if</u> $\exists$ chain of congruences $0 \prec \alpha_1 \prec \alpha_2 \prec \dots \prec 1$ $(*)$
such that $\mathrm{typ}(\alpha_{i+1}, \alpha_i) \neq 1$

$\boxed{\Rightarrow}$ if $\underline{\mathbf{A}}$ satisfies a non-trivial idempotent Mal'cev condition,
then $\underline{\mathbf{A}} \in \mathcal{K}$

Fact $\underline{\mathbf{A}}$ with constants, and

- $\underline{\mathbf{A}}$ is simple (tame) or
- $\underline{\mathbf{A}}$ is 3-element

Then $\underline{\mathbf{A}} \in \mathcal{K}$ <u>iff</u> ~~$(*)$~~ for all minimal α, $\mathrm{typ}(0,\alpha) \neq 1$

non-membership in $\mathcal{K}$

→ studying subreducts of matrix powers

→ ad hoc construction

THE **ANSWER**

FREE ALGEBRAS

- $\underline{\mathbf{I}}$ is "$\underline{(X,A)\text{-free}}$" for $\underline{\mathbf{A}}$ if $\forall$map $\varphi: X \to A$ can be extended to a homomorphism $\hat{\varphi}: \underline{\mathbf{I}} \to \underline{\mathbf{A}}$

  here $X \subseteq I$

  - $\boxed{\text{Example}}$: $\underline{\mathbf{I}} =$ the free algebra for $HSP(\underline{\mathbf{A}})$ over X

    $$\cong Clo_{|X|}(\underline{\mathbf{A}}) \leq \underline{\mathbf{A}}^{A^{|X|}}$$

  $\Rightarrow$ if $|Clo_n(\underline{\mathbf{A}})| \in \mathcal{O}(n^k)$ then $\underline{\mathbf{A}} \notin \mathcal{K}$ (#homos is $\Omega(2^{\sqrt[k]{|\mathbf{I}|}})$)

- $\underline{\mathbf{I}}$ is "$\underline{(X, ab)\text{-free}}$" for $\underline{\mathbf{A}}$ if $\forall$map $\varphi: X \to \{a,b\}$ can be extended to a homomorphism $\hat{\varphi}: \underline{\mathbf{I}} \to \underline{\mathbf{A}}$

  $\{a,b\} \subseteq A$, $a \neq b$

  - $\boxed{\text{Example}}$ $\underline{\mathbf{I}} = \{ f \restriction_{\{a,b\}^{|X|}} : f \in Clo_{|X|}(\underline{\mathbf{A}}) \} \leq \underline{\mathbf{A}}^{\{a,b\}^{|X|}}$

  $\Rightarrow$ if $|$"$Clo_n(\underline{\mathbf{A}}) \restriction_{\{a,b\}}$"$| \in \mathcal{O}(n^k)$ then $\underline{\mathbf{A}} \notin \mathcal{K}$

Is it a standard concept?

NON-MEMBERSHIP IN $\mathcal{K}$

Def $\alpha \in \mathrm{Con}(\underline{\mathbf{A}})$ is <u>strongly abelian</u> if

$$f(x_0, x_1, \dots, x_{n-1}) = f(y_0, y_1, \dots, y_{n-1}) \Rightarrow f(x_0, z_1, \dots, z_{n-1}) = f(y_0, z_1, \dots, z_{n-1})$$

whenever $f \in \mathrm{Clo}_n(\underline{\mathbf{A}} + \text{constants})$, $(x_0, y_0) \in \alpha$, $(x_i, y_i) \in \alpha$, $(y_i, z_i) \in \alpha$, $i = 1, \dots, n-1$

α strongly abelian, $(a, b) \in \alpha$, $a \neq b \Rightarrow f\restriction_{\{a,b\}^n}$ depends on at most $\log_2 |A|$ coordinates

$\Rightarrow \left| \text{"} \mathrm{Clo}_n(\underline{\mathbf{A}} + \text{consts})\restriction_{\{a,b\}} \text{"} \right| \in \mathcal{O}(n^{\log_2 |A|}) \Rightarrow \underline{\mathbf{A}} \notin \mathcal{K}$

Remark: enough to have (a,b) generating a strongly rectangular tolerance (we get $\mathcal{O}(n^{|A|})$ instead of $\mathcal{O}(n^{\log_2 |A|})$) [Kearnes, Kiss '13]

THE ANSWER

THEOREM For a finite algebra $\underline{A}$ the following are equivalent.

(1) $\underline{A} \in \mathcal{K}$ $\quad$ (# homos $\underline{I} \to \underline{A}$ $\leq p(|\underline{I}|)$)

(2) no subalgebra of $\underline{A}$ has a nonzero strongly abelian congruence

---

- if $\underline{A} \notin \mathcal{K}$ $\quad$ # homos $\underline{I} \to \underline{A}$ is $\cancel{2^{\Omega(|I|)}}$ $2^{|I|^{\Omega(1)}}$
- $\underline{A}$ finite signature: $\quad$ (2) can be tested in P ; $\quad$ effective enumeration of homos
  - $\underline{A} \in \mathcal{K} \Rightarrow$ CSP over any expansion of $\underline{A}$ is ~~NP-complete~~ in P
  - $\underline{A} \notin \mathcal{K} \Rightarrow$ CSP over some expansion of $\underline{A}$ is NP-complete (1 ternary relation suffices)

QUESTIONS

- was it known/studied?
- complexity of CSP over algebras remains open
- what is $\mathcal{L} = \{\underline{A} ;\ \forall \underline{I} \in HSP(\underline{A})$ has small generating set$\}$?

THANK YOU