The number of homomorphisms into finite algebras

Libor Barto, Charles University, Czechia

+ William DeMeo
Antoine Mottet

Feb 10, 2022 TCS lab seminar, HSE University, Russia

CoCoSym: Symmetry in Computational Complexit

This project has received funding from the European Research Council (ERC) under the European Union Horizon 2020 research and innovation program (grant agreement No 771005

THE QUESTION

- Fix a set A of size 16

  \# mappings $X \longrightarrow A$ $= 16^n$ ... exponential

  set of size n

- Fix a group $\underline{A}$ of size 16

  \# homomorphisms $\underline{X} \longrightarrow \underline{A}$ $\leq n^4$ ... polynomial

  group of size n
  algebra of size n

  = # ways $\underline{A}$ is "contained in $\underline{X}$" as a quotient

- **Question:** For which algebras $\underline{A}$ is # homomorphisms $\underline{X} \to \underline{A} \leq \text{poly}(|X|)$?

  finite
  finite

OUTLINE

- algebras, homomorphisms
- origin of the question
- examples + ideas
- answer

INTERRUPT!

ALGEBRAS, HOMOMORPHISMS

- algebra = universe + operations on the universe

  e.g. $\underline{A} = (A;\ \bullet^{\underline{A}},\ i^{\underline{A}},\ 1^{\underline{A}})$

  $\bullet^{\underline{A}} : A \times A \longrightarrow A$ binary operation on A

  $i^{\underline{A}} : A \longrightarrow A$ unary

  $1^{\underline{A}} \in A$ constant

  $\underline{X} = (X;\ \bullet^{\underline{X}},\ i^{\underline{X}},\ 1^{\underline{X}})$ similar algebra

- homomorphism $f : \underline{X} \to \underline{A}$ = mapping $X \to A$ preserving operations

$$f(x \bullet^{\underline{X}} y) = f(x) \bullet^{\underline{A}} f(y)$$
$$f(i^{\underline{X}}(x)) = i^{\underline{A}}(f(x))$$
$$f(1^{\underline{X}}) = 1^{\underline{A}}$$

THE ORIGIN

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

  INPUT: $\mathbb{X}$ ... similar structure

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

- covers many computational problems (e.g. 3SAT, 3COLORING)
- complexity classification $<^{P}_{NP}$ [Bulatov'17; Zhuk'17]
- method: algebra

- CSP over $\underline{A}$ ... algebra

  INPUT: $\underline{X}$ ... similar algebra

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

- covers more computational problems
- complexity classification open
- "often": in P for simple reason

  ... we can list all homomorphisms in polynomial time

  $\rightsquigarrow$ the question

QUESTION: For which $\underline{A}$

$$\forall \underline{X} \quad \# \underline{X} \to \underline{A} \leq \mathrm{poly}(|X|) \ ?$$

EXAMPLE : GROUPS

- $\underline{A} = (A;\ \cdot^{\underline{A}},\ i^{\underline{A}},\ 1^{\underline{A}})$ group

$$a\cdot(b\cdot c) = (a\cdot b)\cdot c \qquad \forall a,b,c \in A$$
$$a\cdot 1 = a = 1\cdot a$$
$$a\cdot i(a) = 1 = i(a)\cdot a$$

- $\underline{X} = (X;\ \cdot^{\underline{X}},\ i^{\underline{X}},\ 1^{\underline{X}})$ group / general $\rightsquigarrow$ can enforce identities true in $\underline{A}$

$\boxed{\text{EXAMPLE: NOR}}$

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

$\cdot^{\underline{A}}$	0	1
0	1	0
1	0	0

consider $a * b := (x \cdot y) \cdot ((x \cdot x) \cdot (y \cdot y))$

what is $a *^{\underline{A}} b$?

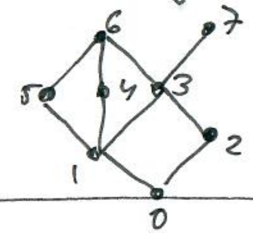
$\rightsquigarrow$ can add term operations

EXAMPLE : SEMILATTICE

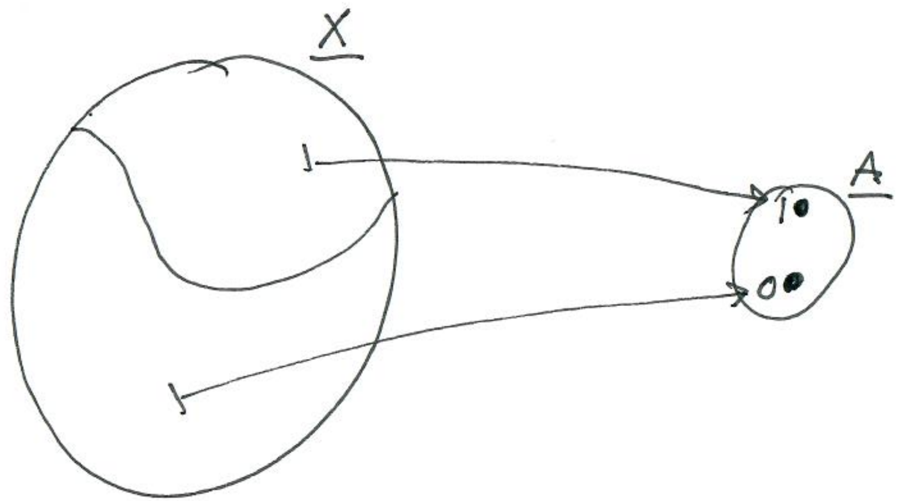
- $\underline{A} = (\{0,1\}; \bullet^{\underline{A}})$ $\quad a \bullet^{\underline{A}} b := \min(a,b)$

semilattice $\underline{S} = (S, \bullet^{\underline{S}})$ $\quad s \bullet^{\underline{S}} r = \inf(s,r)$ w.r.t. some ordering on S

or $\begin{cases} s(rt) = (sr)t \\ ss = s \\ sr = rs \end{cases}$



- WLOG $\underline{X}$ is a semilattice
- consider $f: \underline{X} \to \underline{A}$



$\boxed{\text{EXAMPLE : MAJORITY}}$

- $\underline{A} = (\{0,1\};\ m^{\underline{A}})$ $\qquad m^{\underline{A}}(0,0,0) = m^{\underline{A}}(1,0,0) = m^{\underline{A}}(0,1,0) = m^{\underline{A}}(0,0,1) = 0$
  $\qquad m^{\underline{A}}(1,1,1) = m^{\underline{A}}(0,1,1) = m^{\underline{A}}(1,0,1) = m^{\underline{A}}(1,1,0) = 1$

- consider $f : \underline{X} \to \underline{A}$ — not onto / onto

  - if $f(\mathbf{s}) = 0$ then f preserves $\qquad s^{\underline{A}}(x,y) := m^{\underline{A}}(0,x,y) \quad x,y \in A$
    $\qquad s^{\underline{X}}(x,y) := m^{\underline{X}}(\mathbf{s},x,y) \quad x,y \in X$

    such an s exists

  - $s^{\underline{A}}$ is min!

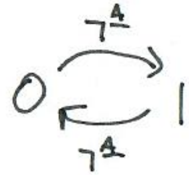
$\rightsquigarrow$ 0 can add constants to A

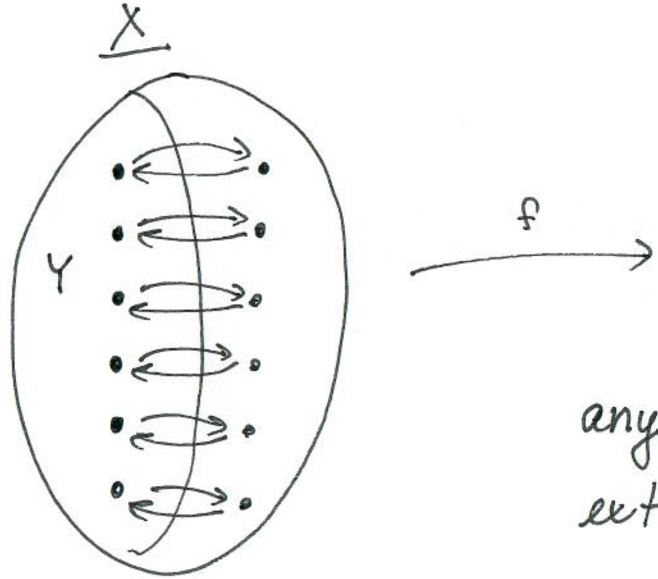
EXAMPLE: UNARY

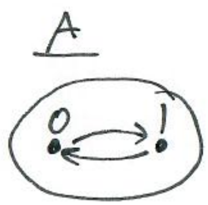
not polynomial

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

a	0	1
$\neg^{\underline{A}}$	1	0







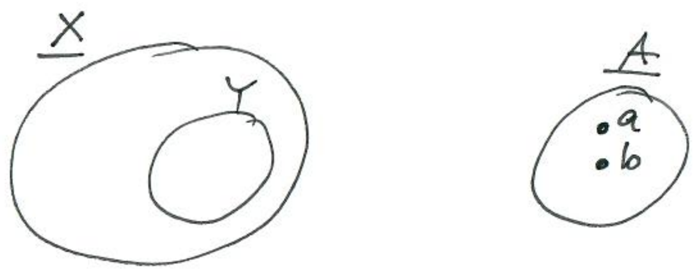
any mapping $Y \to \{0,1\}$
extends to homomorphism

- $\bigcirc$s, these examples, Post $\to$ sufficient to answer the question for $|A|=2$
  $|A|=2$, contains only essentially unary operations ... exponentially many homomorphisms
  $|A|=2$, doesn't — " — ... polynomially many
- for $|A|>2$, the Tame Congruence Theory useful [Hobby, McKenzie '88 + ...]

MANY HOMOMORPHISMS

- For some $\underline{A}$ there exists arbitrarily large $\underline{X}$ such that
  - $\exists Y \subseteq X$ large (eg. $|Y| \geq |X|^{\frac{1}{37}}$)
  - any mapping $Y \to \{a, b\}$ extends to a homomorphism $\underline{X} \to \underline{A}$

    some specific elements of A



- Then $\# \underline{X} \to \underline{A} \not\leq \mathrm{poly}(|X|)$

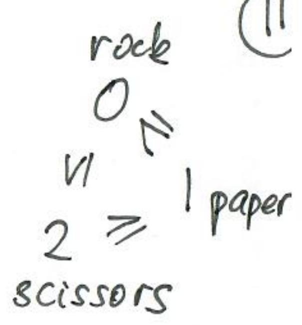
- Turns out: otherwise $\# \underline{X} \to \underline{A} \leq \mathrm{poly}(|X|)$!

EXAMPLE: ROCK-PAPER-SCISSORS

polynomial

$a \cdot^{A} b$ = looser

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



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

- take $\underline{X}$, $f: \underline{X} \to \underline{A}$
- consider $p(x) = x.0$

a	0	1	2
$p^{A}(a)$	0	0	2

- $Z := p^{\underline{X}}(X)$ $\overset{!!!}{\Rightarrow}$ $f(Z) \subseteq \{0,2\}$

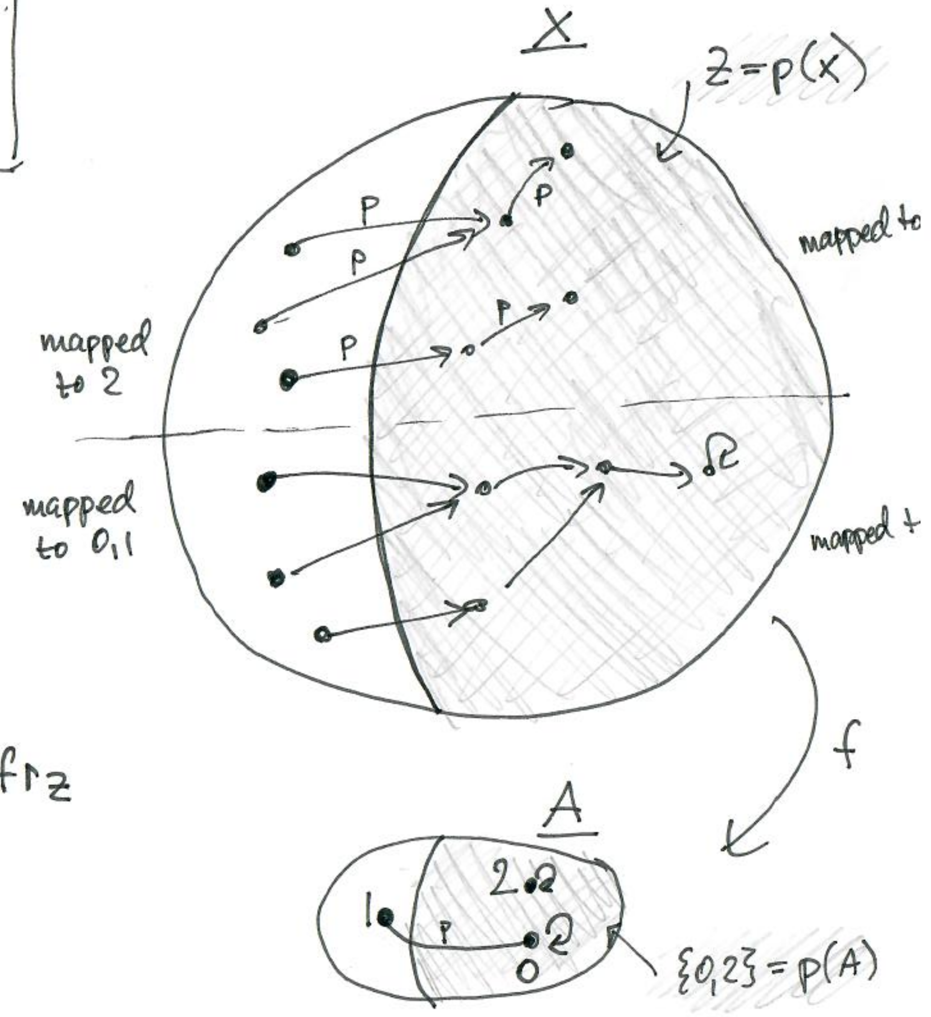
  $\rightsquigarrow$ polynomially many $f \restriction Z$

- Fix $f \restriction Z$ for $x \in X$

  if $f \restriction Z\,(p(x)) = 2$ then $f(x) = 2$

  if $ = 0$ then $f(x) \in \{0,1\}$

  $\rightsquigarrow$ polynomially many extensions of $f \restriction Z$



THE ANSWER

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

(1) $\# \underline{X} \to \underline{A} \leq \mathrm{poly}(|X|)$

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

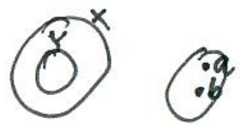
---

(2) • depends on term operations of $\underline{A}$

• can be tested in P (given $\underline{A}$ on input)

• if (2) then, given $\underline{X}$, all homomorphisms $\underline{X} \to \underline{A}$ can be listed in P

if $\neg(2)$ • there exist $\underline{X}$'s such that $\# \underline{X} \to \underline{A} \geq 2^{|X|^{\frac{1}{k}}}$ constant depending on $\underline{A}$

for the simple reason 

• complexity of CSP over $\underline{A}$ still open in general

THANK YOU!