Algebra & Logic in the Complexity of Constraints

Libor Barto

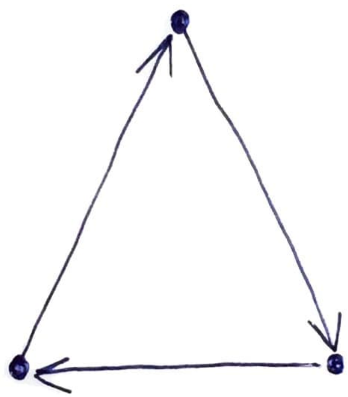
LC'22

CoCosym: Symmetry in Computational Complexity

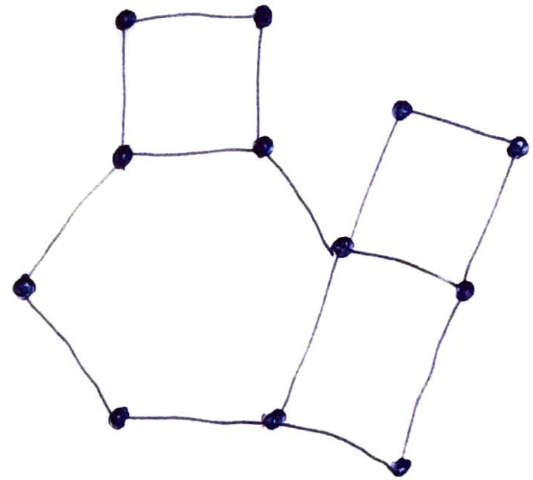
This project has received funding from the European Research Council (ERC) under the European Union Horizon 2020 research and innovation program (grant agreement No 771005)

Are these shapes symmetric ?

1



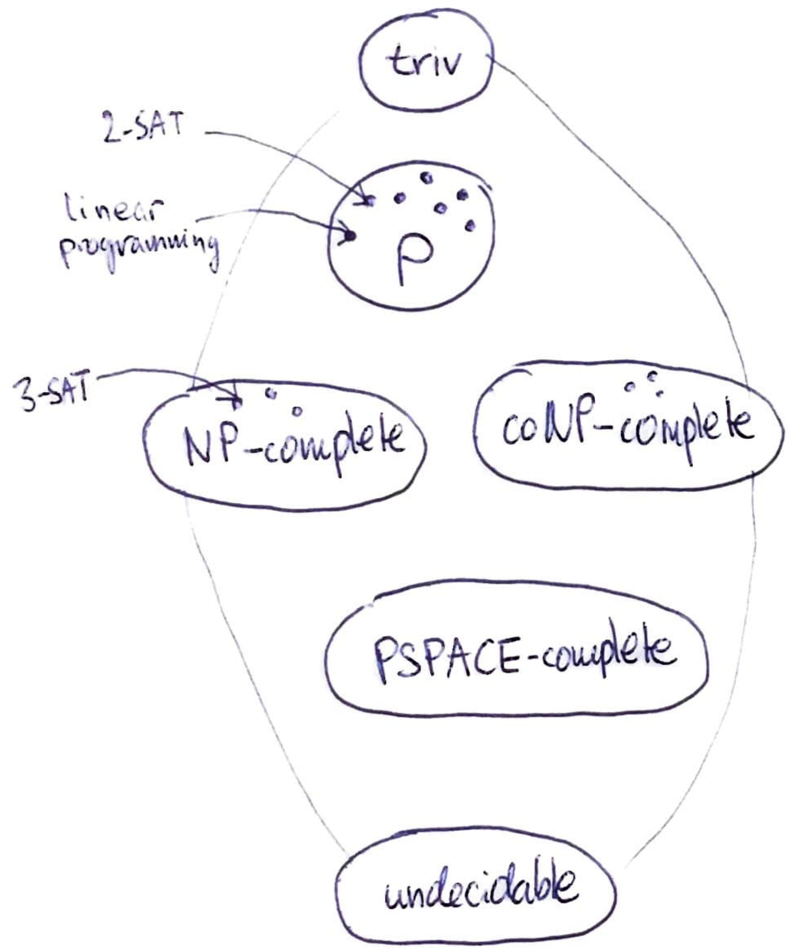
2



3

coffee

What makes computational problems easy / hard?



Answer: Symmetry / lack thereof
(work in progress... ☺)

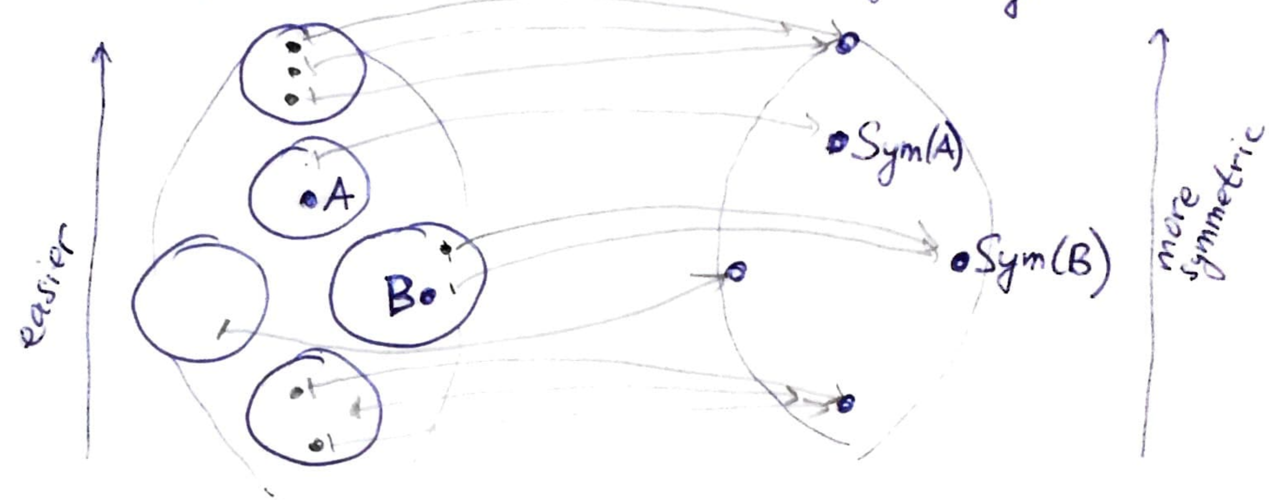
Objections:

- too optimistic
  - true in "CSPs" + way beyond
  - but necessary

fixed-template finite-domain constraint satisfaction problems

- I don't care
  - neither did I
  - maybe interested in desribing structures up to ...

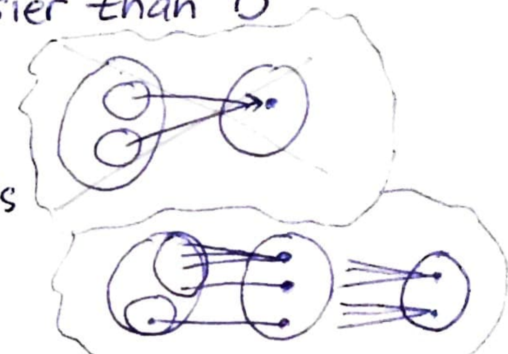
Strategy



- Ideally $\quad Sym(A) \geq Sym(B) \iff A$ easier than B

  ie. A is more symmetric than B

- Approach
  - find Sym such that $\Longrightarrow$ holds
  - abstract (forget some info)



- Traditionally $\quad$ object $\xmapsto{sym}$ permutation group $\xmapsto{abstraction}$ abstract group

- CSPs $\quad$ CSP $\xmapsto{sym}$ clone $\xmapsto{abstraction}$ abstract group $\xmapsto{abstraction}$

  $\longmapsto$ abstract minion $\xmapsto{abstr.}$ ...

OUTLINE

- Clones
- Constraint Satisfaction Problems (CSPs)
- Promise CSPs

notation

$\mathbb{A} = (A; R, S)$ relational structure with domain A and relations $R \subseteq A^k$, $S \subseteq A^\ell$

$\underline{A} = (A; f, g)$ algebra with domain A and operations $f: A^k \to A$, $g: A^\ell \to A$

different rôles

CLONES

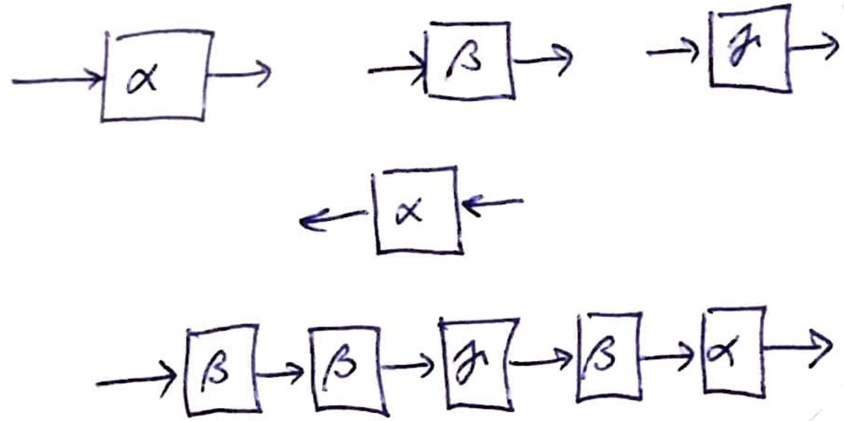
$\boxed{\text{Clones}}$

permutation group on A

$\mathcal{G}$ .. set of ~~unary~~ bijective operations $A \to A$

closed under inverses and term-definable unary operations:

e.g. $\alpha, \beta, \gamma \in \mathcal{G} \Rightarrow \psi \in \mathcal{G}$
where $\psi(x) = \alpha(\beta(\gamma(\beta(\beta(x)))))$

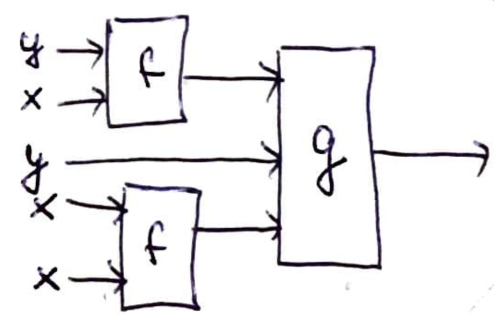


transformation monoid on A ~~bijective~~ ~~closed under inverses~~

clone on A moreover ~~unary~~

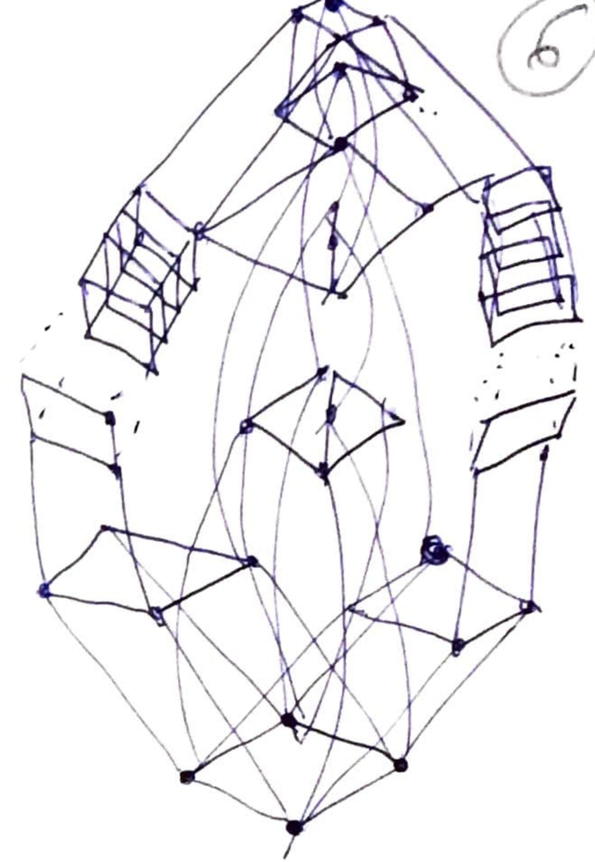
$\mathcal{C}$ .. set of operations $A^n \to A$
closed under term-definable operations

e.g. $f: A^2 \to A,\ g: A^3 \to A \Rightarrow h: A^2 \to A \in \mathcal{C}$ where
$h(x,y) = g(f(y,x), y, f(x,x))$



Why study clones

- $A = \{0,1\}$ expressive power of logical connectives
  [Post'41 The two-valued iterative systems of math. logic 122 pp.]
  full classification
- $|A| > 2$ dtto for multiple-valued logic
- $\underline{A}$ algebra $\mathrm{Clo}(\underline{A})$ = all term-definable operations
  – important invariant



Post's lattice

Ex.
- $\mathrm{Clo}(\{0,1\};\ \min(x,y)) = \mathrm{Clo}(\{0,1\};\ \mathrm{AND}(x,y)) = ?$
- $\mathrm{Clo}(\{0,1\};\ \min, \max) = ?$
- $\mathrm{Clo}(\{0,1\};\ x+y+z \bmod 2) = ?$
- $\mathrm{Clo}(\{0,1\};\ \mathrm{majority}(x,y,z)) = ?$
- $\mathrm{Clo}(\{0,1\};\ \_\_\_) = ?$
- $\mathrm{Clo}(\{0,1\};\ \mathrm{AND}(x,y), \mathrm{OR}(x,y), \neg(x)) = ?$

Fun ex: $\mathrm{Clo}(\{0,1\};\ \to)$

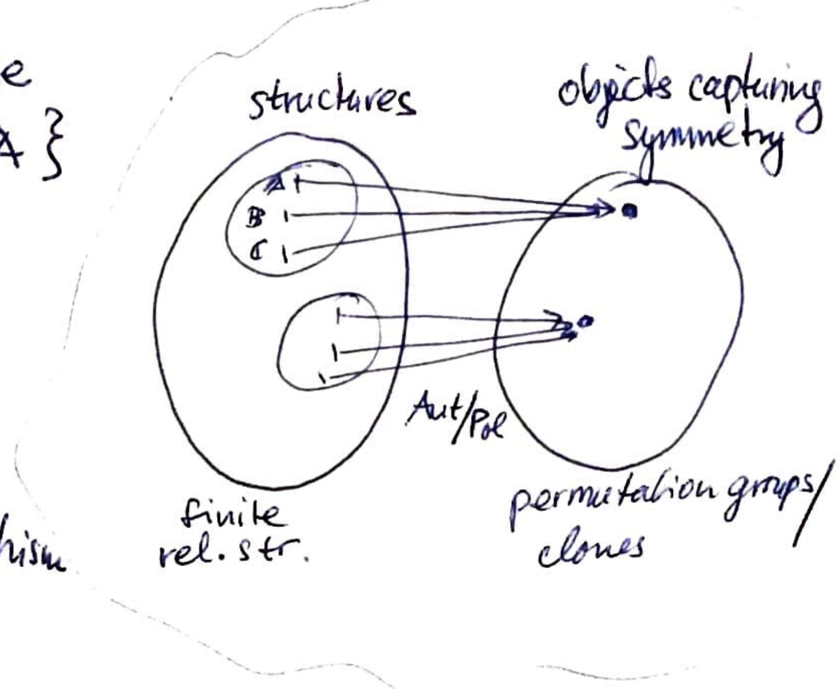
- object capturing symmetry

Polymorphisms

or more or less whatever

$\mathbb{A} = (A;\ R, S, \dots)$ relational structure, say A finite

- $\mathbb{A} \longmapsto \mathrm{Aut}(\mathbb{A}) = \{ f : A \to A;\ f \text{ is invertible homomorphism } \mathbb{A} \to \mathbb{A} \}$



★ what does this invariant capture?

i.e. when $\mathrm{Aut}(\mathbb{A}) = \mathrm{Aut}(\mathbb{B})$?

when $\mathrm{Aut}(\mathbb{A}) \subseteq \mathrm{Aut}(\mathbb{B})$?

- $\mathbb{A} \longmapsto \mathrm{Pol}(\mathbb{A}) = \{ f : A^n \to A;\ f \text{ is a homomorphism } \mathbb{A}^n \to \mathbb{A} \}$

i.e. $\begin{pmatrix} \\ \\ \end{pmatrix} \begin{pmatrix} \\ \\ \end{pmatrix} \begin{pmatrix} \\ \\ \end{pmatrix} \cdots \begin{pmatrix} \\ \\ \end{pmatrix} \overset{f}{\longmapsto} \begin{pmatrix} \\ \\ \end{pmatrix}$

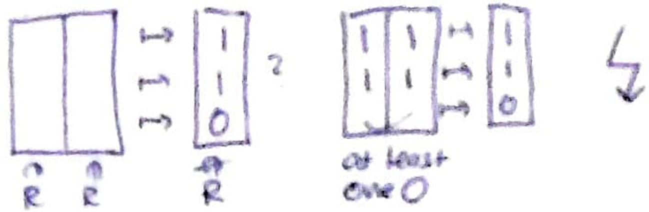
$\ \ \ \ \ \ \in R \ \ \ \in R \ \ \cdots \ \ \in R \ \ \Rightarrow \ \ \in R$

Ex $\mathrm{Pol}(\{0,1\};\ x \leq y)$ - $\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \overset{\longmapsto}{\longmapsto} \begin{pmatrix} f(0,0,1,0) \\ f(0,1,1,1) \end{pmatrix}$ $\quad f(0,0,1,0) \leq f(0,1,1,1)$

$\ \ \in \leq \ \ \ \in \leq \ \ \ \in \leq \ \ \ \in \leq \qquad\qquad \in \leq$

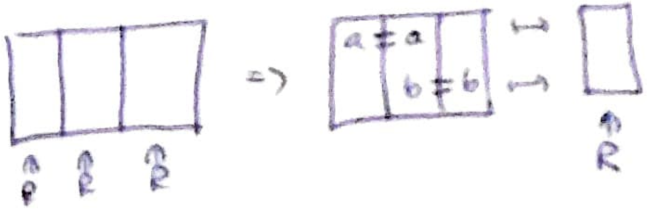
Polymorphisms – examples

- $\mathrm{Pol}(\{0,1\}; x \leq y) =$ monotone $\{0,1\}^n \to \{0,1\} = \mathrm{Clo}(\{0,1\}; \min(x,y), \max(x,y))$
- $\min(x,y) \in \mathrm{Pol}(\{0,1\}; x \wedge y \to z)$



in fact $\mathrm{Pol}(\{0,1\}; x \wedge y \to z, x = 0) =$
$= \mathrm{Clo}(\{0,1\}; \min(x,y))$

- $\mathrm{majority}(x,y,z) \in \mathrm{Pol}(\{0,1\};$ all binary relations$)$



in fact $= \mathrm{Clo}(\{0,1\}; \mathrm{majority}(x,y,z))$
$=$ monotone, $\neq$-preserving operations

- $\mathrm{Pol}(\{0,1\};$ 1-in-3$)$ 1-in-3 $= \left\{ \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \right\}$

  - if $f(1,0,\dots,0) = 1$
    $f(0,0,\dots,0) = 0$

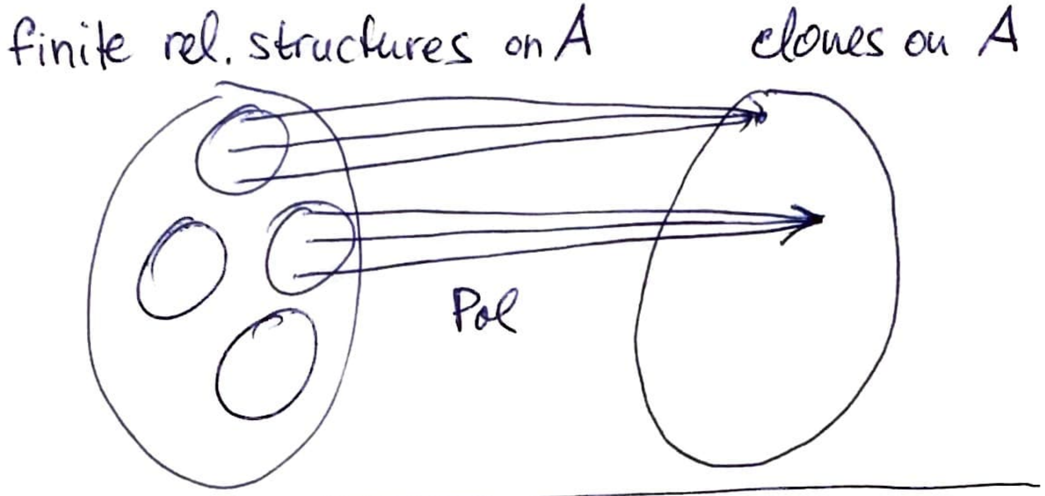
$\dots$ $f(x_1, \dots, x_n) = x_1$

  - ....

$=$ projections

- $\mathrm{Pol}(\mathbb{A})$ is a clone + for finite A, each clone is such [Geiger 68, Bodnarčuk, Kalužnin, Kotov, Romov 69]

What do polymorphisms capture?



also say "$\mathbb{B}$ is pp-definable from $\mathbb{A}$"

Theorem $\mathrm{Pol}(\mathbb{A}) \subseteq \mathrm{Pol}(\mathbb{B}) \iff$ each relation in $\mathbb{B}$ is pp-definable from $\mathbb{A}$ [Geiger '68, Bodnarčuk, Kalužnin, Kotov, Romov '68]

pp-definable = definable using $\exists, \wedge, =,$ relations in $\mathbb{A}$

e.g. $S(x,y,z) \overset{def}{\equiv} \exists u\ \exists v\ R(x,u) \wedge R(v,y) \wedge z=u$

Proof:
- one direction easy
- second direction: beautiful abstract nonsence

$\exists$ Version for ∞ [Bodirsky, Nešetřil]

Clones summary

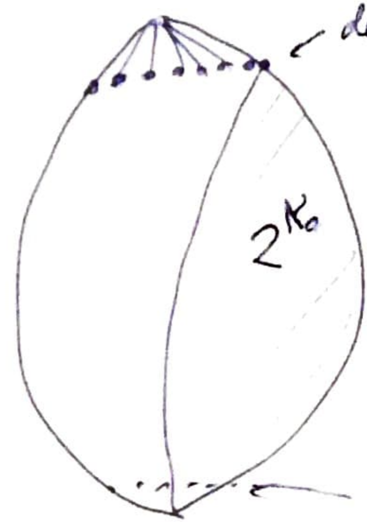
- objects capturing symmetry, finer than permutation groups
- clones on A $=$ sets of propositional connectives / expressibility

  $=$ algebras / term equivalence

  $=$ relational structures / pp-definability

- $|A| = 2$
- $|A| > 2$ general pessimism, but e.g.

  $2^{\aleph_0}$



CSP

$\boxed{\text{CSP}}$

fixed structure, say $\mathbb{A} = (A;\ \underbrace{R, S}_{\text{binary}})$

$\text{CSP}(\mathbb{A})$

– deciding $\exists\wedge$= sentences in $\mathbb{A}$

constraints

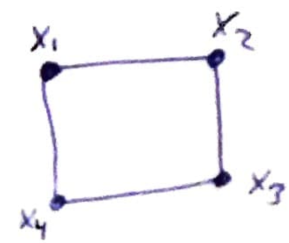
INPUT: pp-sentence, e.g. $\varphi = \exists x_1 \exists x_2 \dots\ R(x_1, x_3) \wedge S(x_5, x_2) \wedge R(x_3, x_1) \wedge \dots$

ANSWER YES: φ satisfied in $\mathbb{A}$

ANSWER NO: φ not satisfied in $\mathbb{A}$

Ex $\mathbb{A} = (\{\text{red}, \text{green}, \text{blue}\};\ x \neq y) = \mathbb{K}_3$

INPUT: e.g. $\exists\ x_1 \neq x_2 \wedge x_2 \neq x_3 \wedge x_3 \neq x_4 \wedge x_1 \neq x_4$ $\mathbb{X}$



YES $\Leftrightarrow$ $\mathbb{X}$ 3-colorable

in NP for finite $\mathbb{A}$

- $|A| = 2$ P/NP-complete dichotomy [Schaeffer '78]
- $\mathbb{A}$ finite graphs [Hell, Nešetřil '90]
- [Feder, Vardi '98] interesting for $|A| > 2$, dichotomy conjecture
- [Bulatov '17, Zhuk '17] dichotomy theorem for $|A| < \aleph_0$

CSP examples

- CSP($\{0,1\}$; $x \vee y \vee z$, $x \vee y \vee \neg z$, ...) = 3-SAT

  input e.g. $\exists x_1 \exists x_2 \dots (x_3 \vee x_1 \vee \neg x_2) \wedge (\neg x_5 \vee x_{37} \vee x_{\lceil e\pi \rceil}) \wedge \dots$
- CSP($\{0,1\}$; $x \vee y$, $x \vee \neg y$, $\neg x \vee \neg y$) = 2-SAT
- CSP($\{0,1\}$; $x \wedge y \to z$, ~~z~~ $x=0$) = HORN-3-SAT
- CSP($\{0,1\}$, 1-in-3) = 1-in-3-SAT
- CSP($\{0,1\}$; $x+y+z=0$, $x+y+z=1 \pmod 2$) = $\mathbb{Z}_2$-LINEAR EQUATIONS
- CSP($\{0,1,2\}$; $\neq$) = 3-COLORING
- CSP($\{0,1\}$; ternary "not-all-equal") = NAE-3-SAT

  = 3-UNIFORM HYPERGRAPH 2-COLORING

MOTIVATION

- covers interesting problems
- now: starting point for THE STRATEGY
- descriptive complexity... [Feder, Vardi]
  - alternative definition $CSP(\mathbb{A})$ INPUT: $\mathbb{X}$ of the same signature
    OUTPUT: $\mathbb{X} \xrightarrow{\text{homo}} \mathbb{A}$?
    (see the coloring example)
  - can $\{\mathbb{X};\ \mathbb{X} \to \mathbb{A}\}$ be described in some logic (nice logic ⇝ easy problem)

[Fagin'73] NP = existential 2nd order logic.
[FV] MMSNP = CSP
exploring the quest of logic capturing P [Gurevich'88 ?]

$\boxed{\mathbb{A} = \{0,1\}}$ [Schaeffer '78]

0. $\mathbb{A}$ pp-definable from $\mathbb{B} \Rightarrow$ CSP($\mathbb{A}$) easier than CSP($\mathbb{B}$)

- if $\mathbb{A}$ pp-definable from $(\{0,1\}; x \vee y, x \vee \neg y)$
  $\Rightarrow$ CSP($\mathbb{A}$) easier than ~~HORN 3-SAT~~ 2-SAT $\Rightarrow$ in P
- — " — HORN-3-SAT — " —
- — " — $\mathbb{Z}_2$-LINEAR EQUATIONS — " —
- 2 more trivial cases
- else: NP-hard why:
  - pick $\mathbb{B}$ such that CSP($\mathbb{B}$) NP-hard
  - show that $\mathbb{A}$ pp-definable from $\mathbb{B}$
  - deduce CSP($\mathbb{A}$) NP-hard (0. again)

e.g. CSP(1-in-3) NP-hard since "3-SAT" pp-definable from 1-in-3

how to pp-define 3-SAT from 1-in-3

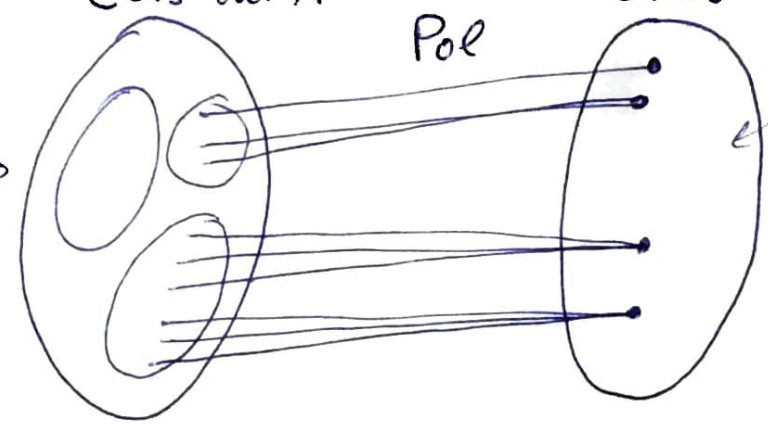
- work hard & be creative
- .... wait.... this sounds familiar

Symmetries for CSPs = algebraic reality (known as "approach")

[Jeavons et al '00]

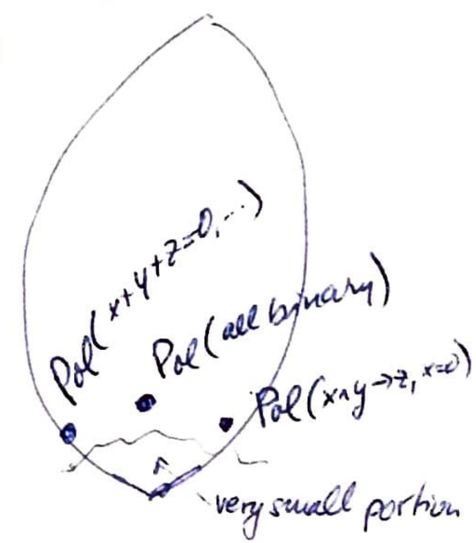
+ Theorem: $\mathrm{Pol}(\mathbb{A}) \supseteq \mathrm{Pol}(\mathbb{B}) \Rightarrow$ CSP($\mathbb{A}$) easier than CSP($\mathbb{B}$)

- success in the 1st step of THE STRATEGY



coffee

- Pol($\mathbb{A}$) higher in the Post lattice (CSP($\mathbb{A}$) more symmetric)
  $\Rightarrow$ CSP($\mathbb{A}$) easier
- Schaeffer could start from bottom and go up
  - would hit P very soon
  - would not need to be creative & work hard (Post did)
    eg. 1-in-3-SAT hard since Pol(1-in-3) = projections

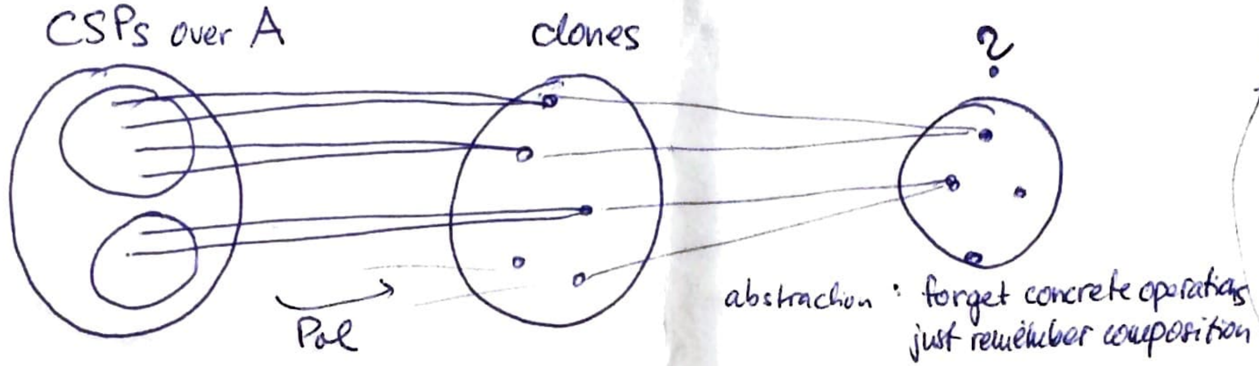


- ☹ $|A|>2$ we don't have description of clones …

Abstraction

beer →

- .... we need to continue THE STRATEGY



② = abstract clones (modulo clone homomorphic equivalence) $\mathcal{C} \leftrightarrows \mathcal{D}$

compare to groups

- Recall: $\mathrm{Pol}(\mathbb{A}) \subseteq \mathrm{Pol}(\mathbb{B}) \iff \mathbb{B}$ pp-definable from $\mathbb{A}$
  & then CSP($\mathbb{B}$) easier than CSP($\mathbb{A}$)
- Now: $\boxed{\exists\, \mathrm{Pol}(\mathbb{A}) \xrightarrow{\text{clone homo}} \mathrm{Pol}(\mathbb{B}) \iff \mathbb{B} \text{ pp-interpretable in } \mathbb{A}}$
  & still CSP($\mathbb{B}$) easier than CSP($\mathbb{A}$)

mapping preserving term definitions, e.g. $f(x,y) = g(x, h(y,x))$
$\Rightarrow \bar{f}(x,y) = \bar{g}(x, \bar{h}(y,x))$

= preserving identities, e.g. associative commutative operation is mapped to —"—

☺ can use rich theory of algebras & identities: universal algebra

☹ need to learn it

☺ no longer need to fix A

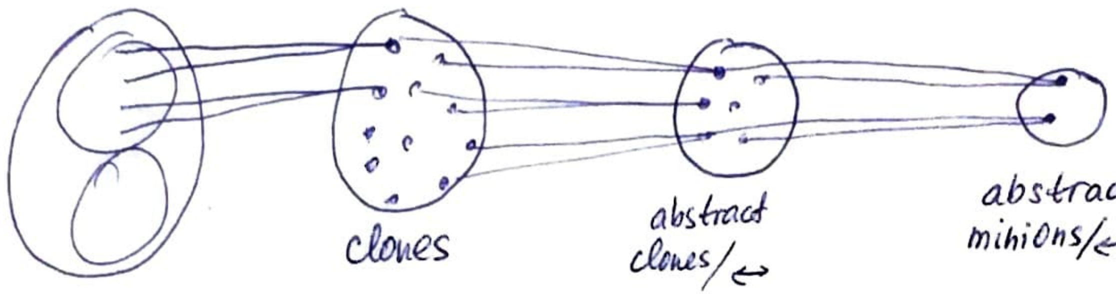
☺ Zhuk didn't & still proved the dichotomy

Further abstraction

"Wonderland of reflections" [B., Opršal, Pinsker '18]

$\mathbb{A} \xrightarrow{\text{pp-power}} \mathbb{C} \xrightarrow{\text{homo}} \mathbb{B}$ (homomorphically equivalent)

simple concept!



$\exists\, \mathrm{Pol}(\mathbb{A}) \xrightarrow{\text{minion homo}} \mathrm{Pol}(\mathbb{B}) \Longleftrightarrow \mathbb{B}$ pp-constructible from $\mathbb{A}$

& still $\mathrm{CSP}(\mathbb{B})$ easier than $\mathrm{CSP}(\mathbb{A})$

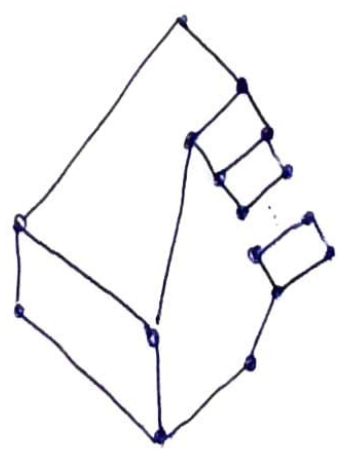
preserves "simplest" term definitions, e.g. $f(x,y) = g(x,y,x) \Rightarrow \bar{f}(x,y) = \bar{g}(x,y,x)$

without complexity:

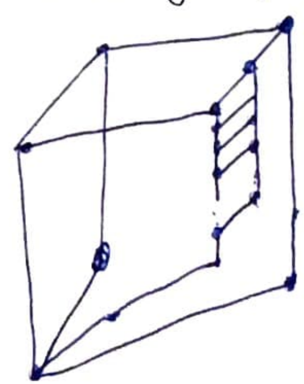
structures / pp-def. / pp-int. / pp-cons.

= clones / Δ / $\xleftrightarrow{\text{clone homo}}$ / $\xleftrightarrow{\text{minion homo}}$

☺ 2-elements [Bodirsky, Vucaj '20]



☺ part on 3-elements [Bodirsky, Vucaj, Zhuk]



maybe can be desribed! ☺ little known

☺ still not ☹

but

single element!

CSP TODOs

finnished 3rd ballpoint pen

- understand dichotomy proofs
- further abstraction until !
- finer complexity / descriptive complexity classification (L, NL, ...)
- logic for P within CSP
- generalizations / variants
  - different quantifiers, connectives $\subseteq \{\exists, \forall, \neg, =, \neq, \wedge, \vee\}$
    only one left: QCSP $(\forall, \exists, \wedge, =)$
    - trichotomy conjecture
    - $\geq$ heptachotomy [Martin, Zhuk '21]
  - valued relations (instead of $\subseteq A^n$ consider $A^n \to \mathbb{R} \cup \{\infty\}$)
  - infinite domains
  - Promise CSP

PCSP

$\boxed{\text{PCSPs}}$

→ fixed structures such that $\mathbb{A} \to \mathbb{B}$

$\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$

INPUT: pp-sentence φ

YES: φ satisfied in $\mathbb{A}$

NO: φ not satisfied in $\mathbb{B}$

search version

INPUT: pp-sentence φ satisfied in $\mathbb{A}$

FIND: satisfying assignment in $\mathbb{B}$

☺ includes concrete problems of major interest in CS

e.g. $\mathrm{PCSP}(\mathbb{K}_3, \mathbb{K}_6)$ = 6-coloring a 3-colorable graph (complexity open)

$\mathrm{Pol}(\mathbb{A}, \mathbb{B}) = \{ f : \mathbb{A}^n \to \mathbb{B} \}$

☺ still captures complexity

☹ it is not a clone, it is a minion

$f \in \mathcal{M} \Rightarrow g \in \mathcal{M}$ where $g(x,y) = f(x,y,x,x)$

☺ — " —

☺ abstraction works

☺ it is not enough < new tools / great opportunity for THE STRATEGY

WRAP UP

- $\exists$ higher-arity symmetries & are useful
- permutation group $\rightarrow$ abstract group
  clone $\rightarrow$ abstract clone $\rightarrow \dots \rightarrow \dots$
- join us!
  - can use a lot of math
  - but can start right away
  - both: fundamental problems / concrete projects
  - practical advantages

Reading

- B, Krokhin, Willard: Polymorphisms and How to Use Them
- + other paper in this Dagstuhl volume
- M. Bodirsky: Complexity of Infinite-domain Constraint Satisfaction
- B, Bulín, Krokhin, Opršal: Algebraic Approach to Promise Constraint Satisfaction

polymorphism

ignore

bleed