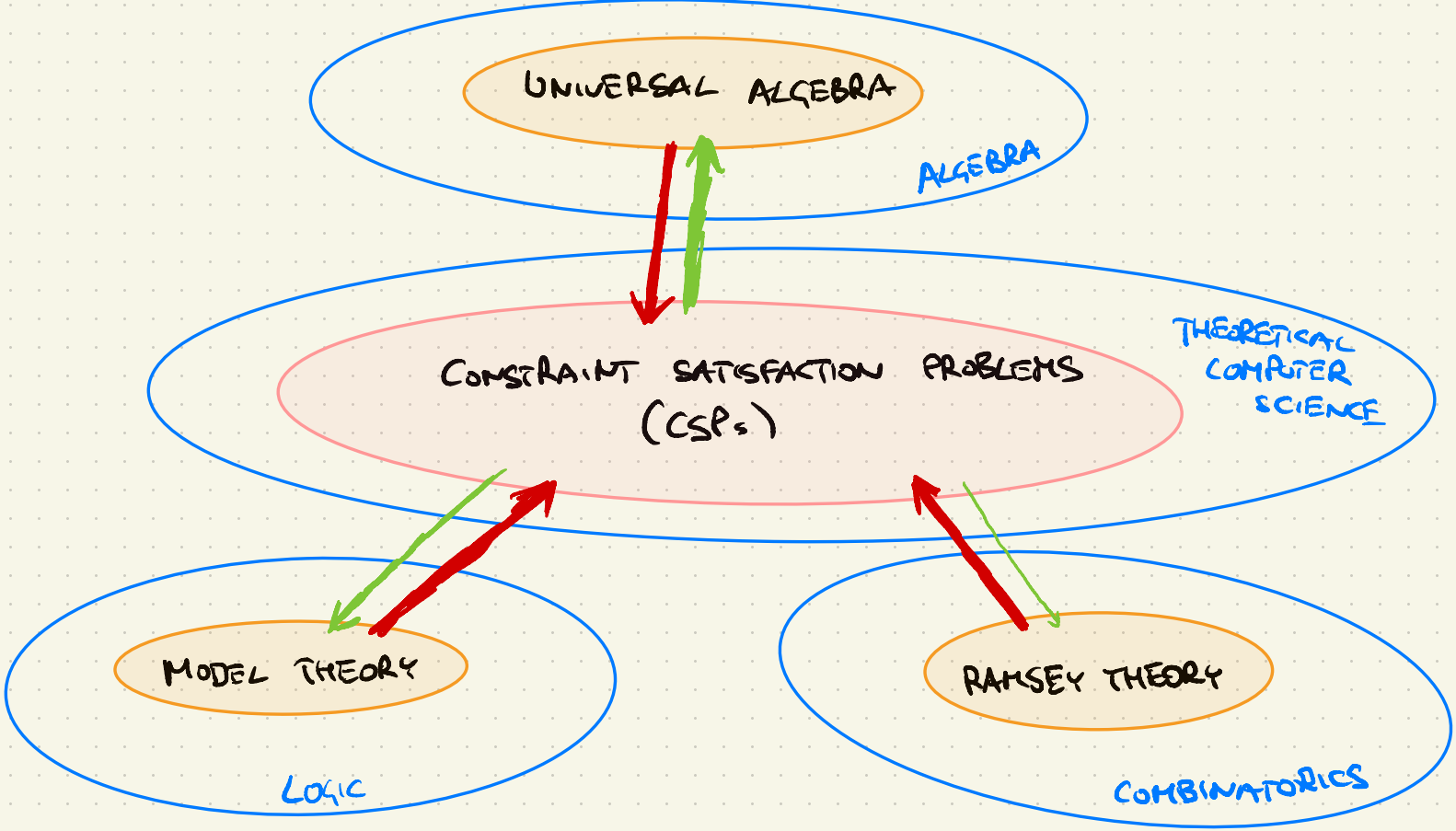
ALGEBRAIC, LOGICAL & COMBINATORIAL METHODS FOR CONSTRAINT SATISFACTION PROBLEMS (CSPs)

MICHAEL PINSKER

PURE MATHEMATICS COLLOQUIUM
UNIVERSITY OF WATERLOO
5.4.2021


UNIVERSAL ALGEBRA
ALGEBRA
CONSTRAINT SATISFACTION PROBLEMS
(CSPs)
THEORETICAL COMPUTER SCIENCE
MODEL THEORY
LOGIC
RAMSEY THEORY
COMBINATORICS

CSP (CONSTRAINT SATISFACTION PROBLEM):

COMPUTATIONAL PROBLEM:

INPUT: VARIABLES + "CONSTRAINTS"

Q: $\exists$ SOLUTION?

COMPLEXITY?

MOST IMPORTANTLY, (FOR US) TIME COMPLEXITY (IN # OF VARIABLES)

EXAMPLES

- GIVEN EQUATIONS (OVER A RING, FIELD ...)

  $\exists$ SOLUTION?

  - DIOPHANTINE EQUATIONS (OVER $(\mathbb{Z}, +, \cdot, 0, 1)$)

    UNDECIDABLE

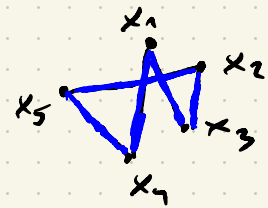
  - LINEAR EQUATIONS (E.G. OVER $(\mathbb{Q}, +, \cdot, 0, 1)$ OR $(\mathbb{Z}_p, +, \cdot, 0, 1)$)

    POLYNOMIAL TIME

MORE EXAMPLES

- GIVEN VARIABLES, SOME "CONNECTIONS" BETWEEN THEM

  (A.K.A. GRAPH)



Q: IS THERE A 3-COLORING?

(VARIABLES ASSIGNED VALUES IN $\{0,1,2\}$, NO ADJACENT VARIABLES GET SAME COLOR)

EXPONENTIAL TIME

NP-COMPLETE :- HARD TO FIND SOLUTION

- EASY TO CHECK SOLUTION

Q: IS THERE A 2-COLORING?

$\in$ P (POLYNOMIAL TIME)

MORE EXAMPLES

- GENERALIZED SUDOKU ($n^2 \times n^2$ GRID)

  NP-COMPLETE

- 3-SAT

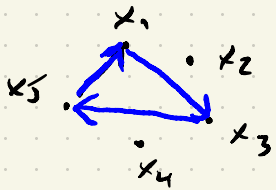
  GIVEN EXPRESSION

  $$\underbrace{(x_1 \vee \neg x_2 \vee x_3)}_{3} \wedge \underbrace{(\neg x_1 \vee x_2 \vee x_4)}_{3} \wedge \dots \wedge$$

  NP-COMPLETE

  Q: SATISFIABLE ?

- GIVEN DIGRAPH (VARIABLES + DIRECTED "CONNECTIONS")



  Q: CAN VARIABLES BE TOTALLY ORDERED SUCH THAT

  $$\forall i,j \quad x_i \to x_j \Rightarrow x_i \leq x_j$$

  $\in P$ "ACYCLICITY"

COMMON ABSTRACTION:

$\mathbb{A} = (A; R_1, \dots, R_m)$ RELATIONAL STRUCTURE

SET = "DOMAIN" RELATIONS ON DOMAIN

CSP($\mathbb{A}$)

INPUT: SENTENCE

$$\varphi = \underbrace{\exists x_1 \dots \exists x_n}_{\text{VARIABLES}} R_{i_1}(\text{SOME VARIABLES}) \wedge R_{i_2}(\text{SOME VARIABLES}) \wedge \dots R_{i_\ell}(\text{SOME VARIABLES})$$

Q: $\mathbb{A} \models \varphi$?

EXAMPLES

- $(\mathbb{Z}, +, \cdot, 0, 1)$
- $(\mathbb{Z}_p, +, \cdot, 0, 1)$ ($+, \cdot$ AS TERNARY RELATIONS)
- $(\mathbb{Q}, +, 0, 1)$
- $(\mathbb{Z}_p, +, 0, 1)$
- $(\{0,1\}, \neq)$
- $(\{0,1\}, \text{ALL 3-ARY REL.})$
- $(\mathbb{Q}, <)$
- $(\{0,1,2\}, \neq)$

- $\mathbb{A}$ INFINITE: $CSP(\mathbb{A})$ ⋮ UNDECIDABLE, NP-c, P, ⋮

EVERY COMPUTATIONAL PROBLEM POLYNOMIAL-TIME EQUIVALENT TO SOME CSP

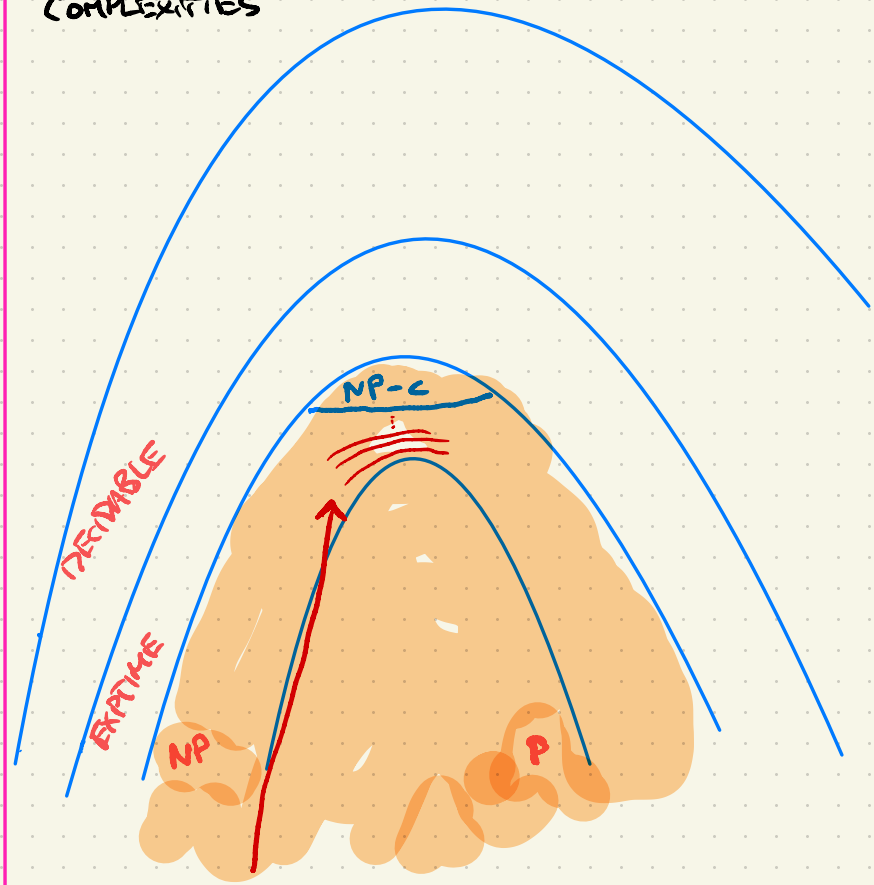
(BODIRSKY + GROHE '07)

- $\mathbb{A}$ FINITE $\Rightarrow$ $CSP(\mathbb{A}) \in$ NP
  - 3-SAT — NP-COMPLETE
  - $(\mathbb{Z}_p, +, 0, 1)$ — P
  - 2-COLORING — P
  - 3-COLORING — NP-c
  - $(\mathbb{Z}_2, +, \cdot, 0, 1)$ — NP-c

1-IN-3-SAT: $x \cdot y = 0$, $x \cdot z = 0$, $y \cdot z = 0$ $\quad (1-x)\cdot(1-y)(1-z) = 0$

$\{(1,0,0), (0,1,0), (0,0,1)\}$

COMPLEXITIES



LADNER'S THEOREM: MANY CLASSES INBETWEEN

CONJECTURE (FEDER + VARDI '93)

$\mathbb{A}$ FINITE $\Rightarrow$ CSP($\mathbb{A}$) — NP-c / P

THEOREM (BULATOV, ZHUK '17)

CONJECTURE TRUE.

GREAT?

- WHY IS THERE A DICHOTOMY?
- WHEN IS A COMPUTATIONAL PROBLEM EASY (P) / HARD (NP-c)?
- WHAT IS SYMMETRY?

$\Longrightarrow$ $\boxed{\text{UNIVERSAL ALGEBRA}}$

EXAMPLES

- CSP($\mathbb{Z}_p, +, 0, 1$)

  EASY BECAUSE OF GAUSS.

  SOLUTIONS: AFFINE SPACE:

  $\bar{u}, \bar{v}, \bar{w}$ SOLUTIONS $\Rightarrow$ $\bar{u} - \bar{v} + \bar{w}$ SOLUTION

  THEREFORE:

  $$m: \mathbb{Z}_p^3 \to \mathbb{Z}_p$$
  $$(x,y,z) \mapsto x - y + z$$

  PRESERVES SOLUTIONS/($\mathbb{Z}_p, +, 0, 1$)

  SYMMETRY: $m(x,x,y) = y = m(y,x,x)$

- CSP($\{0,1\}; <$)

  EASY: LOCAL CHECKING $x_i \to x_j \to x_k$

  SOLUTIONS: $\bar{s}, \bar{t}$ SOLUTIONS $\Rightarrow$ $\max(\bar{s}, \bar{t})$ SOL.

  SYMMETRY: $\max(x,y) = \max(y,x)$, ...

$\mathbb{A} = (A; R_1, \dots, R_m)$ RELATIONAL STRUCTURE

$k \geq 1$

$f: A^k \to A$ <u>POLYMORPHISM</u> $:\Leftrightarrow$

WHENEVER $\bar{r}_1, \dots, \bar{r}_k \in R_i$ FOR SOME i

$\Rightarrow f(\bar{r}_1, \dots, \bar{r}_k) \in R_i$

$\boxed{\mathrm{Pol}(\mathbb{A})}$ ... ALL POLYMORPHISMS OF $\mathbb{A}$

"POLYMORPHISM ALGEBRA"

(DOMAIN: A; FUNCTIONS: POLYMORPHISMS)

SIMILAR TO AUTOMORPHISM GROUP $\mathrm{Aut}(\mathbb{A})$

ENDOMORPHISM MONOID $\mathrm{End}(\mathbb{A})$

DIFFERENT KINDS OF <u>SYMMETRIES</u>

THEOREM (BULATOV + JEAVONS + KROKHIN '05)
(BARTO + OPRŠAL + P. '17)

- $\mathbb{A}, \mathbb{B}$ FINITE, SAME DOMAIN

  $\mathrm{Pol}(\mathbb{A}) = \mathrm{Pol}(\mathbb{B}) \Rightarrow \mathrm{CSP}(\mathbb{A}) \sim \mathrm{CSP}(\mathbb{B})$

  PTIME

- $\mathbb{A}, \mathbb{B}$ FINITE,

  ALL NON-NESTED EQUATIONS SATISFIED IN $\mathrm{Pol}(\mathbb{A})$ ALSO SATISFIED IN $\mathrm{Pol}(\mathbb{B})$

  $\Rightarrow \mathrm{CSP}(\mathbb{B}) \leq \mathrm{CSP}(\mathbb{A})$

  PTIME

"THE <u>RICHER</u> $\mathrm{Pol}(\mathbb{A})$ (IN EQUATIONS), THE <u>EASIER</u> $\mathrm{CSP}(\mathbb{A})$"

SATISFACTION OF EQUATIONS, E.G.

$$m(x,x,y) = m(x,y,x) = m(y,x,x)$$

THERE <u>EXISTS</u> A POLYMORPHISM m FOR WHICH THE EQUATION IS TRUE

POOREST POSSIBLE Pol(𝔸):

ALL PROJECTIONS ON $\{0,1\}$

$\pi(x_1 \dots x_n) = x_i$

$\mathrm{PROJ} = \mathrm{Pol}(\underbrace{\text{1-IN-3SAT}}_{(\{0,1\};\{(0,0,1),(0,1,0),(1,0,0)\})})$

$\mathrm{Pol}(\mathbb{A})$ TRIVIAL $:\Leftrightarrow$ ALL NON-NESTED EQUATIONS OF $\mathrm{Pol}(\mathbb{A})$ ARE TRUE IN PROJ

THEOREM (BULATOV, ZHUK '17)

$\mathbb{A}$ FINITE

$\mathrm{Pol}(\mathbb{A})$

- TRIVIAL → $\mathrm{CSP}(\mathbb{A})$ NP-c
- NON-TRIVIAL → $\mathrm{CSP}(\mathbb{A}) \in P$

THEOREM (MAROTI + MCKENZIE; BARTO + KOZIK; SIGGERS; BARTO + OPRŠAL + P. 2005)

$\mathbb{A}$ FINITE

$\mathrm{Pol}(\mathbb{A})$

- TRIVIAL → NO NON-NESTED EQUATIONS
- NON-TRIVIAL → $\mathrm{Pol}\,\mathbb{A}$ SATISFIES:
  - $w(x,\dots,x,y) = \dots = w(y,x,\dots,x)$

  AND
  - $c(x_1,\dots,x_n) = c(x_2,\dots,x_n,x_1)$

  AND
  - $s(x,y,x,z,y,z) = s(y,x,z,x,z,y)$

  AND
  - $s(a,r,e,a) = s(r,a,r,e)$

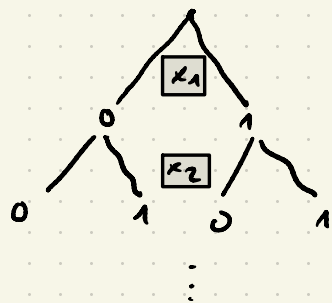
EQUATIONS = SYMMETRIES

EXAMPLE $\mathbb{A} = (\{0,1\}; \dots)$ $\quad \max(x,y) \in \mathrm{Pol}(\mathbb{A})$

CSP($\mathbb{A}$):

INSTANCE: VARIABLES $x_1, \dots, x_n$

+ CONSTRAINTS



EXPONENTIAL!

BUT BECAUSE <u>max</u> IS POLYMORPHISM ....

- CHECK <u>LOCALLY</u> IF $x_1 = 1, \dots x_n = 1$ POSSIBLE
  ↑ ON CONSTRAINTS
- IF NOT ⇒ REDUCED TO SMALLER INSTANCE WITH $x_i := 0$
- IF YES ⇒ $(1, \dots, 1)$ SOLUTION

... IN GENERAL: TOTALLY SYMMETRIC POLYMORPHISMS

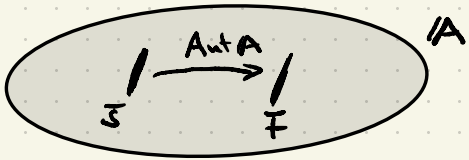
THIS DOES NOT WORK FOR INFINITE $\mathbb{A}$

MODEL THEORY

WANT: CONNECTION

$$\mathrm{CSP}(\mathbb{A}) \Leftrightarrow \mathrm{Pol}(\mathbb{A})$$

$\mathbb{A}$ ω-CATEGORICAL $:\Leftrightarrow$ $\mathbb{A}$ COUNTABLE & $\forall n \geq 1$ $\mathrm{Aut}\,\mathbb{A} \curvearrowright A^n$ HAS FINITELY MANY ORBITS



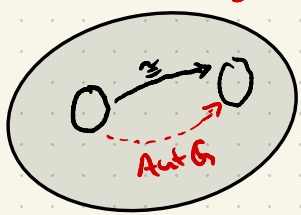
"$A^n / \mathrm{Aut}\,\mathbb{A}$ IS FINITE $\forall n \geq 1$"

CSP: SOLUTION SPACE IS INFINITE

<u>BUT</u> FOR EVERY GIVEN INSTANCE $(x_1 \dots x_n)$ IT IS "<u>FINITE</u>"!

EXAMPLES

- $(\mathbb{Q}, <)$
- RANDOM GRAPH = UNIVERSAL HOMOGENEOUS GRAPH G



- RANDOM POSET
- RANDOM BOOLEAN ALGEBRA = COUNTABLE ATOMLESS BOOLEAN ALGEBRA

⋮

+ ALL STRUCTURES DEFINABLE IN THEM:

E.G. $(\mathbb{Q}, B(x,y,z))$

$B(x,y,z) :\Leftrightarrow x<y<z \vee z<y<x$

$CSP(\mathbb{Q}, B(x,y,z))$:

GIVEN VARIABLES $x_1 \dots x_n$
+ CONSTRAINTS = SPECIFIED TRIPLES

Q: ARE THERE VALUES FOR $x_1 \dots x_n$ IN $\mathbb{Q}$ SUCH THAT ALL CONSTRAINTS SATISFY BETWEENNESS?

NP-COMPLETE

$\mathbb{A}$ DEFINABLE IN HOMOGENEOUS STRUCTURE WITH „REASONABLE DESCRIPTION" (FINITE BOUNDEDNESS)

$\Rightarrow CSP(\mathbb{A}) \in NP$

CONJECTURE MOM

IN THAT CASE:

$Pol(\mathbb{A})$

TRIVIAL $\rightarrow$ $CSP(\mathbb{A})$ NP-c

NON-TRIVIAL $\rightarrow$ $CSP(\mathbb{A}) \in P$

WHAT DOES "TRIVIAL" MEAN HERE?

$\mathrm{Pol}(\mathbb{A})$ TRIVIAL IF $\exists$ FINITE SET S A WHERE ALL NON-NESTED IDENTITIES SATISFIED ARE ALSO SATISFIED IN PROJ.

IN THAT CASE: $\mathrm{CSP}(\mathbb{A})$ is NP-c.

BARTO + OPRŠAL + P. '16

OTHERWISE: $\mathrm{Pol}(\mathbb{A}) \models e \circ s(x,y,x,z,y,z) = f \circ s(y,x,z,x,z,y)$

BARTO + P. '17

BARTO + KOMPATSCHER + OLŠÁK + PHAM + P. '18

METHODS:
- COMPACTNESS
- ORBIT GROWTH

WHY NO SOLUTION TO CONJECTURE?
- EQUATION NOT NICE
- THEORY BEHIND THE EQUATION NOT NICE
- FUNCTION s NOT NICE

RAMSEY THEORY

LET $f: \mathbb{Q} \to \mathbb{Q}$

$\Rightarrow \forall F \subseteq \mathbb{Q}$ FINITE $\exists F' \subseteq \mathbb{Q}$ FINITE $|F| = |F'|$, $f|_{F'}$ is INCREASING OR DECREASING

(RAMSEY'S THEOREM)

$\Rightarrow \overline{\mathrm{Aut}(\mathbb{Q},<) \circ f \circ \mathrm{Aut}(\mathbb{Q},<)}$ ← POINTWISE CLOSURE

CONTAINS DECREASING OR INCREASING FUNCTION

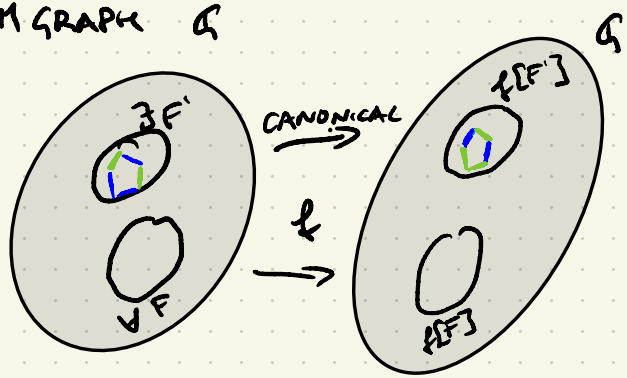
"SAME" FOR $f: \mathbb{Q}^n \to \mathbb{Q}$!

$\overline{\mathrm{Aut}(\mathbb{Q},<) \circ f \circ (\mathrm{Aut}(\mathbb{Q},<))^n}$

IF f is POLYMORPHISM OF $(\mathbb{Q},<)$ $\Rightarrow$ "GENERATES" CANONICAL POLYMORPHISM

ANOTHER EXAMPLE

RANDOM GRAPH G



$\mathrm{Pol}(\mathbb{A})$

TRIVIAL → $\mathrm{CSP}(\mathbb{A})$ NP-c

NON-TRIVIAL → $\mathrm{cons}(x,y,x,z,y,z) =$
$\mathrm{cons}(y,x,z,x,z,y)$

CANONICAL POLYMORPHISMS

TRIVIAL → ?

NON-TRIVIAL → $\mathrm{CSP}(\mathbb{A}) \in$ P

(BODIRSKY + MOTTET '17)

GOOD NEWS:

- CANONICAL POLYMORPHISMS ARE NOT RARE (RAMSEY THEORY) BODIRSKY + P. + TSANKOV '13
- ? OFTEN DOES NOT OCCUR "SMOOTH APPROXIMATIONS METHOD"

THEOREM (MOTTET + P. '20)

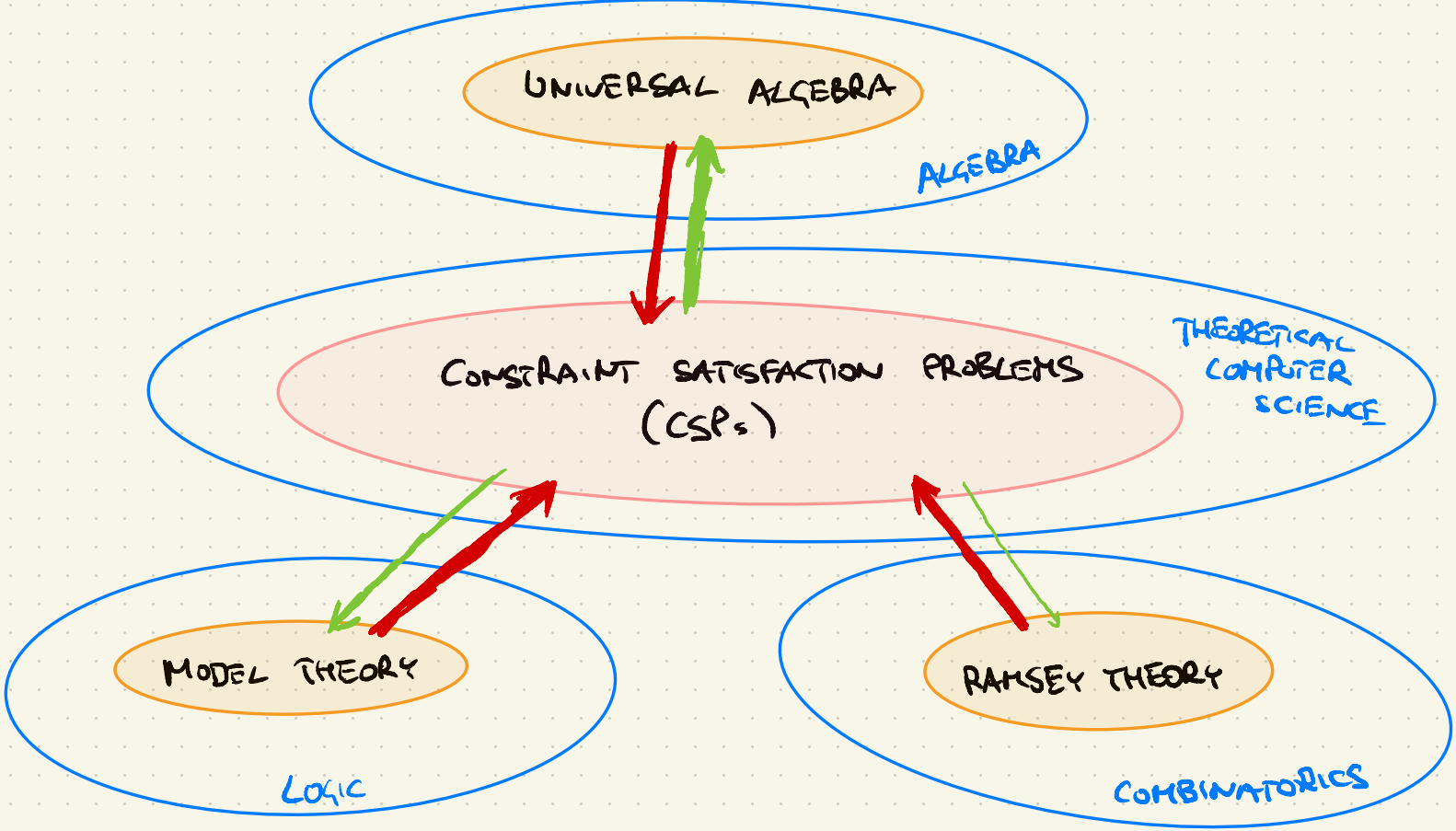
LET $\mathbb{A}$ BE DEFINABLE IN:

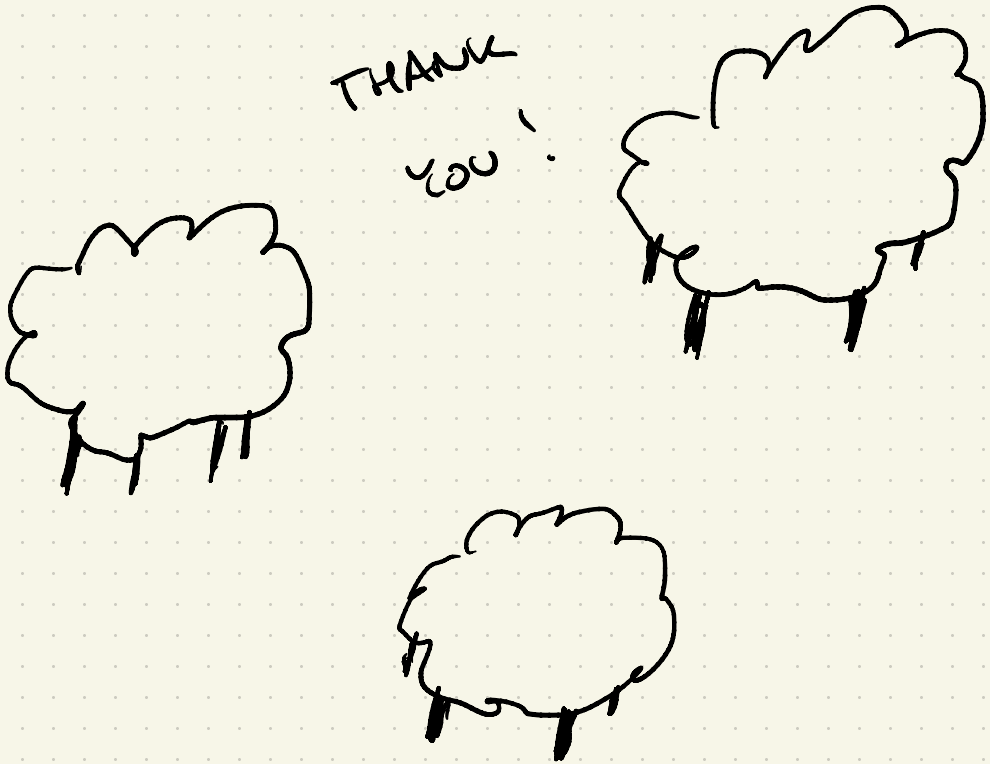
- $(\mathbb{Q},<)$
- RANDOM TOURNAMENT
- HOMOGENEOUS GRAPH
- RANDOM POSET
- ...

$\Rightarrow \mathrm{CSP}(\mathbb{A}) \in$ P OR NP-c

SUMMARY

- CSPs ARE COMMON COMPUTATIONAL PROBLEMS PARAMETRIZED BY RELATIONAL STRUCTURES $\mathbb{A}$
- SYMMETRY OF $\mathbb{A}$ AS MEASURED BY EQUATIONS OF POLYMORPHISM ALGEBRA DETERMINES COMPLEXITY IF $\mathbb{A}$ FINITE. STRUCTURAL DICHOTOMY.
- ALSO WORKS FOR ω-CATEGORICAL $\mathbb{A}$.
- USING RAMSEY THEORY, ONE ASSOCIATES A FINITE ALGEBRA (CANONICAL FUNCTIONS) WITH $\mathrm{Pol}(\mathbb{A})$.
- OFTEN, THIS YIELDS STRUCTURAL DICHOTOMY.


UNIVERSAL ALGEBRA
ALGEBRA
CONSTRAINT SATISFACTION PROBLEMS
(CSPs)
THEORETICAL COMPUTER SCIENCE
MODEL THEORY
LOGIC
RAMSEY THEORY
COMBINATORICS


THANK YOU!