Tutorial – The Constraint Satisfaction Problem Dichotomy Theorem. Lecture 1

Ross Willard

Waterloo (Canada)

Assoc. Sym. Logic meeting – Ames, IA
15 May 2024

Plan

1. (Today) The CSP dichotomy theorem (Bulatov & Zhuk).
   - Constraint satisfaction problems
   - Statement of the Dichotomy Theorem
   - "Algebraic" perspective
   - Hopefully accessible to everyone.
2. (Tomorrow) Algebraic idea # 1 from Zhuk's proof
   - Still relatively accessible, but more technical. (Bring coffee)
3. (Friday) Algebraic idea # 2 from Zhuk's proof
   - Very technical, assumes some universal algebra. (You've been warned)

Part 1 – Constraint Satisfaction Problems

M fixed structure: relational, finite, and finite signature.

φ formula over **M**

- $\wedge$at-fmla – conjunction of atomic formulas
- pp-fmla – $\exists\vec{y}\psi$ where ψ is $\wedge$at

$\varphi^{\mathbf{M}}$ – the *n*-ary relation defined in **M** by $\varphi(x_1, \ldots, x_n)$.

Fine print: formulas may contain parameters from **M**.

M fixed structure: relational, finite, and finite signature.

φ formula over **M**

- $\wedge$at-fmla – conjunction of atomic formulas
- pp-fmla – $\exists \vec{y} \psi$ where ψ is $\wedge$at

$\varphi^{\mathbf{M}}$ – the *n*-ary relation defined in **M** by $\varphi(x_1, \ldots, x_n)$.

Constraint Satisfaction Problem $\mathrm{CSP}_p(\mathbf{M})$

(Fix **M**.) $\mathrm{CSP}_p(\mathbf{M})$ is the following decision problem:

Input: $\wedge$at-fmla φ (in signature of **M**)

Question: Is $\varphi^{\mathbf{M}} \neq \varnothing$?

Fine print: formulas may contain parameters from **M**.

$\text{CSP}_p(\mathbf{M})$ can be easy or hard

Example 1: $\mathbf{M}_{3SAT} = (\{0,1\}, R_{3SAT})$ where

$$R_{3SAT} = \{(x_1,\ldots,x_6) \,:\, (x_1,x_2,x_3) \neq (x_4,x_5,x_6)\}.$$

$\mathrm{CSP}_p(\mathbf{M})$ can be easy or hard

Example 1: $\mathbf{M}_{3SAT} = (\{0,1\}, R_{3SAT})$ where

$$R_{3SAT} = \{(x_1,\dots,x_6) : (x_1,x_2,x_3) \neq (x_4,x_5,x_6)\}.$$

$$R_{3SAT}(x,y,z,0,0,0) \quad \text{encodes} \quad x \vee y \vee z$$
$$R_{3SAT}(x,y,z,0,0,1) \quad \text{encodes} \quad x \vee y \vee \neg z, \quad \textit{etc.}$$

CSP$_p$(**M**) can be easy or hard

Example 1: $\mathbf{M}_{3SAT} = (\{0,1\}, R_{3SAT})$ where

$$R_{3SAT} = \{(x_1,\dots,x_6) : (x_1,x_2,x_3) \neq (x_4,x_5,x_6)\}.$$

$$\begin{array}{lll} R_{3SAT}(x,y,z,0,0,0) & \text{encodes} & x \vee y \vee z \\ R_{3SAT}(x,y,z,0,0,1) & \text{encodes} & x \vee y \vee \neg z, \quad etc. \end{array}$$

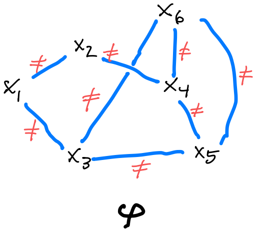
Instances of 3-SAT can be encoded as $\wedge$at-fmlas over $\mathbf{M}_{3SAT}$.

$\therefore$ we have a poly-time reducton 3-SAT $\leq_P$ CSP$_p$($\mathbf{M}_{3SAT}$).

$\therefore$ CSP$_p$($\mathbf{M}_{3SAT}$) is NP-hard, hence NP-complete.

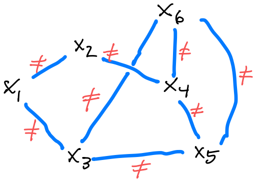
Example 2: $\mathbf{K}_3 = (\{0,1,2\}, \neq)$.

(=-free, parameter-free) $\wedge$at-fmlas in this signature can be pictured; e.g.,



Example 2: $\mathbf{K}_3 = (\{0,1,2\}, \neq)$.

(=-free, parameter-free) $\bigwedge$at-fmlas in this signature can be pictured; e.g.,



φ

$$\varphi^{\mathbf{K}_3} \neq \varnothing \iff \exists \text{ assignment } \{x_1, \ldots, x_6\} \to \{0,1,2\} \text{ preserving } \neq$$
$$\iff \text{this graph can be 3-colored.}$$

$\rightsquigarrow$ polytime reduction 3-COL $\leq_P$ CSP$_p(\mathbf{K}_3)$.

$\therefore$ CSP$_p(\mathbf{K}_3)$ is NP-complete.

Example 3: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

How hard Is $\mathrm{CSP}_p(\mathbf{K}_{2,\leq})$?

Example 3: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

How hard Is $\mathrm{CSP}_p(\mathbf{K}_{2,\leq})$?

Exercize: not hard

$\wedge$at-fmlas over $\mathbf{K}_{2,\leq}$ can't "express" very much.

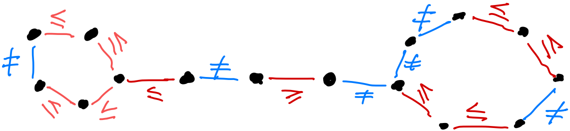
Example 3: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

How hard Is $\mathrm{CSP}_p(\mathbf{K}_{2,\leq})$?

Exercize: not hard

$\wedge$at-fmlas over $\mathbf{K}_{2,\leq}$ can't "express" very much.

$\varphi^{(\mathbf{K}_{2,\leq})} = \varnothing \iff \varphi$ contains a certain kind of "configuration"; in the worst case, one of the form



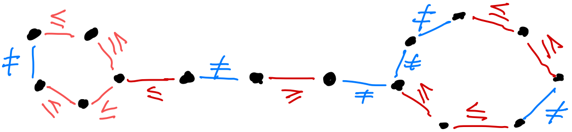
Example 3: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

How hard Is $\mathrm{CSP}_p(\mathbf{K}_{2,\leq})$?

Exercize: not hard

$\wedge$at-fmlas over $\mathbf{K}_{2,\leq}$ can't "express" very much.

$\varphi^{(\mathbf{K}_{2,\leq})} = \varnothing \iff \varphi$ contains a certain kind of "configuration"; in the worst case, one of the form



We can efficiently test whether any such configurations occur in φ.

$\therefore$ $\mathrm{CSP}_p(\mathbf{K}_{2,\leq})$ is in P.

Example 4: $\mathbf{M}_{3lin} = (\{0,1,2\},\ R)$ where

$$R = \{(x,y,z,w) : x - y + z = w \pmod 3\}.$$

Atomic formulas over $\mathbf{M}_{3lin}$ express (short) linear equations/$\mathbb{Z}_3$:

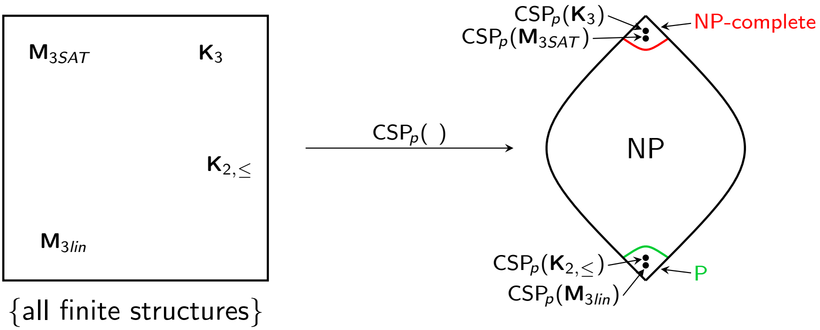
$R(x,y,z,w)$	$x - y + z - w = 0$
$R(x,y,z,1)$	$x - y + z = 1$, etc

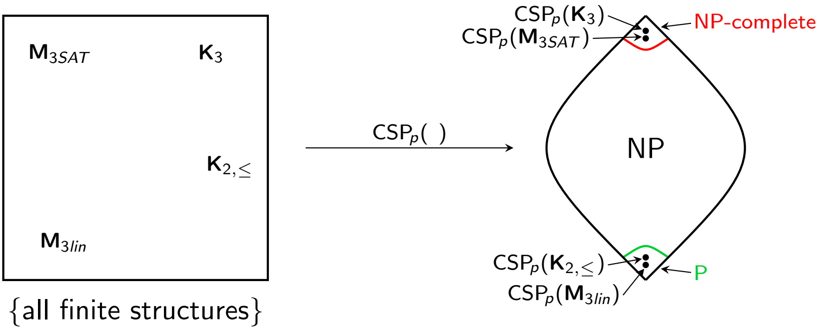
So $\wedge$at-fmlas over $\mathbf{M}_{3lin}$ express (certain) systems of linear equations/$\mathbb{Z}_3$.

We can solve such systems in poly time.

$\therefore$ $\mathrm{CSP}_p(\mathbf{M}_{3lin})$ is in P.

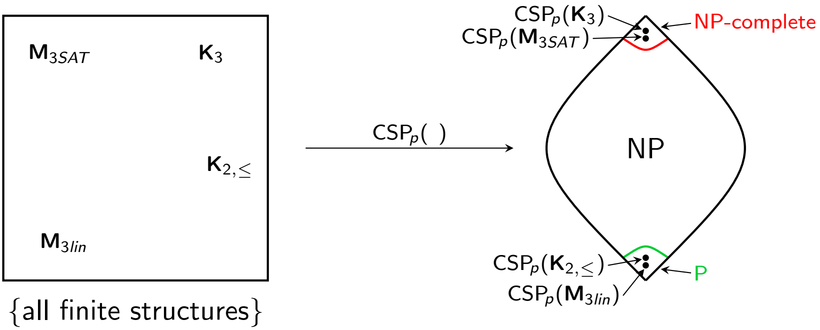
Part 2 – The Dichotomy Theorem


$\mathbf{M}_{3SAT}$
$\mathbf{K}_3$
$\mathbf{K}_{2,\leq}$
$\mathbf{M}_{3lin}$
{all finite structures}
$\mathrm{CSP}_p(\ )$
$\mathrm{CSP}_p(\mathbf{K}_3)$
$\mathrm{CSP}_p(\mathbf{M}_{3SAT})$
NP-complete
NP
$\mathrm{CSP}_p(\mathbf{K}_{2,\leq})$
$\mathrm{CSP}_p(\mathbf{M}_{3lin})$
P



CSP Dichotomy Conjecture (Feder, Vardi 1998)

For every $\mathbf{M}$, CSP$_p(\mathbf{M})$ is in P or is NP-complete.



CSP Dichotomy Conjecture (Feder, Vardi 1998)

For every $\mathbf{M}$, $\mathrm{CSP}_p(\mathbf{M})$ is in P or is NP-complete.

Plausible (in 1998).

- Known for 2-element structures (Schaefer 1978)
- Known for core graphs (Hell, Nešetřil 1990)

(Where should the "dividing line" be?)

pp-interpretations

There is one "obvious" reason for $\mathrm{CSP}_p(\mathbf{M})$ to be NP-complete:

If $\mathbf{M}_{3SAT}$ (or $\mathbf{K}_3$) is $\boxed{\text{pp-interpretable}}$ in $\mathbf{M}$.

"pp-interpretation" means the usual thing:

> There is a pp-definable set $D \subseteq \mathbf{M}^n$, a pp-definable equivalence relation E on D with two blocks (so $E \subseteq \mathbf{M}^{2n}$), and a pp-definable 6-ary relation R on D (so $R \subseteq \mathbf{M}^{6n}$) such that
> $$(D/E,\, R/E) \cong \mathbf{M}_{3SAT}.$$

(A.k.a. "gadget definition.")

pp-interpretations

There is one "obvious" reason for $\mathrm{CSP}_p(\mathbf{M})$ to be NP-complete:

If $\mathbf{M}_{3SAT}$ (or $\mathbf{K}_3$) is pp-interpretable in $\mathbf{M}$.

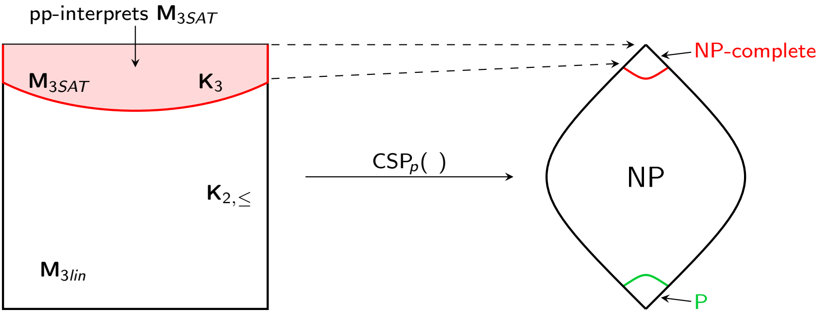
"pp-interpretation" means the usual thing:

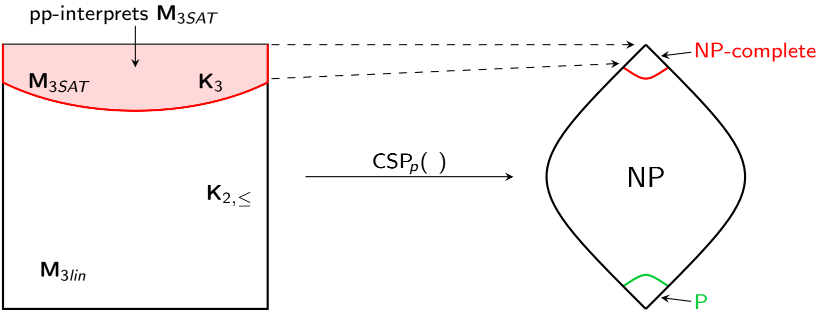
> There is a pp-definable set $D \subseteq \mathbf{M}^n$, a pp-definable equivalence relation E on D with two blocks (so $E \subseteq \mathbf{M}^{2n}$), and a pp-definable 6-ary relation R on D (so $R \subseteq \mathbf{M}^{6n}$) such that
>
> $$(D/E,\, R/E) \cong \mathbf{M}_{3SAT}.$$

(A.k.a. "gadget definition.")

Easy Fact

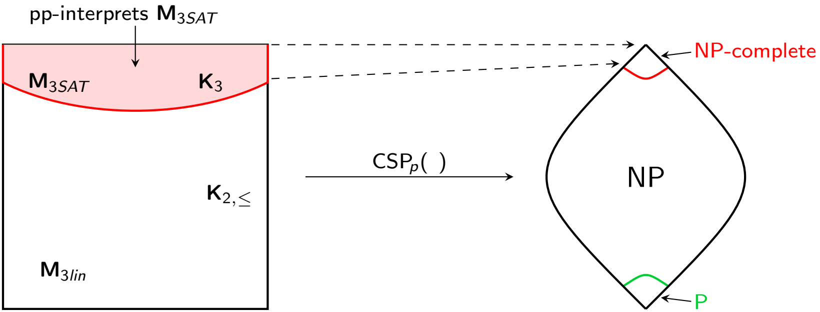
If $\mathbf{M}_{3SAT} \xhookrightarrow{pp} \mathbf{M}$, then $\mathrm{CSP}_p(\mathbf{M})$ is NP-complete.


pp-interprets $\mathbf{M}_{3SAT}$
$\mathbf{M}_{3SAT}$
$\mathbf{K}_3$
$\mathbf{K}_{2,\leq}$
$\mathbf{M}_{3lin}$
$\mathrm{CSP}_p(\ )$
NP
NP-complete
P



Refined Dichotomy Conjecture (Bulatov, Jeavons, Krokhin 2001)

If $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$, then $\mathrm{CSP}_p(\mathbf{M})$ is in P.



Refined Dichotomy Conjecture (Bulatov, Jeavons, Krokhin 2001)

If $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$, then $\mathrm{CSP}_p(\mathbf{M})$ is in P.

The race is on!
Lots of partial results!
Frenetic activity!
Conferences! Workshops! Grant money! And then ...

Part 3 – The Dichotomy Theorem

The Refined Conjecture is proved!

CSP Dichotomy Theorem (A. Bulatov, D. Zhuk 2017; 2020.)

If $\mathbf{M}$ is finite and $\mathbf{M}_{3SAT} \overset{pp}{\not\to} \mathbf{M}$, then $\mathrm{CSP}_p(\mathbf{M})$ is in P.

It was fun while it lasted.

Part 4 – The algebraic perspective

Example: $\mathbf{M} = (M,\ R)$ with arity$(R) = 2$.

Endomorphism of $\mathbf{M}$: any map $f : M \to M$ satisfying

$$\begin{pmatrix} a \\ b \end{pmatrix} \in R \implies \begin{pmatrix} f(a) \\ f(b) \end{pmatrix} \in R.$$

Example: $\mathbf{M} = (M, R)$ with arity$(R) = 2$.

Endomorphism of $\mathbf{M}$: any map $f : M \to M$ satisfying

$$\binom{a}{b} \in R \implies \binom{f(a)}{f(b)} \in R.$$

Definition

A **polymorphism** of $\mathbf{M}$ is any map $f : M^n \to M$ satisfying

$$\binom{a_1}{b_1}, \ldots, \binom{a_n}{b_n} \in R \implies \binom{f(a_1, \ldots, a_n)}{f(b_1, \ldots, b_n)} \in R.$$

"f preserves R"

Example: $\mathbf{M} = (M, R)$ with arity$(R) = 2$.

Endomorphism of $\mathbf{M}$: any map $f : M \to M$ satisfying

$$\begin{pmatrix} a \\ b \end{pmatrix} \in R \implies \begin{pmatrix} f(a) \\ f(b) \end{pmatrix} \in R.$$

Definition

A **polymorphism** of $\mathbf{M}$ is any map $f : M^n \to M$ satisfying

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}, \dots, \begin{pmatrix} a_n \\ b_n \end{pmatrix} \in R \implies \begin{pmatrix} f(a_1, \dots, a_n) \\ f(b_1, \dots, b_n) \end{pmatrix} \in R.$$

"f preserves R"

Example: monotone boolean functions = polymorphisms of $(\{0,1\}, \leq)$.

(Similarly for relations of higher arity, or $\mathbf{M}$ with more than one relation.)

Example: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

- What endomorphisms does it have?

Example: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

- What endomorphisms does it have? (Only id)

Example: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

- What endomorphisms does it have? (Only id)
- Does $\mathbf{K}_{2,\leq}$ have any 2-ary polymorphisms?

Example: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

- What endomorphisms does it have? (Only id)
- Does $\mathbf{K}_{2,\leq}$ have any 2-ary polymorphisms? If $f(x,y)$ is one:

$$f(0,0) \neq f(1,1) \quad \text{and} \quad f(0,0) \leq f(1,1)$$

Example: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

- What endomorphisms does it have? (Only id)
- Does $\mathbf{K}_{2,\leq}$ have any 2-ary polymorphisms? If $f(x,y)$ is one:

$$f(0,0) \neq f(1,1) \quad \text{and} \quad f(0,0) \leq f(1,1)$$

$$\Longrightarrow \quad f(0,0) = 0 \quad \text{and} \quad f(1,1) = 1$$

Example: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

- What endomorphisms does it have? (Only id)
- Does $\mathbf{K}_{2,\leq}$ have any 2-ary polymorphisms? If $f(x,y)$ is one:

$$f(0,0) \neq f(1,1) \quad \text{and} \quad f(0,0) \leq f(1,1)$$

$$\Longrightarrow \quad f(0,0) = 0 \quad \text{and} \quad f(1,1) = 1$$

Also $f(0,1) \neq f(1,0)$.

Example: $\mathbf{K}_{2,\le} = (\{0,1\}, \neq, \le)$.

- What endomorphisms does it have? (Only id)
- Does $\mathbf{K}_{2,\le}$ have any 2-ary polymorphisms? If $f(x,y)$ is one:

$$f(0,0) \neq f(1,1) \quad \text{and} \quad f(0,0) \le f(1,1)$$

$$\implies \quad f(0,0) = 0 \quad \text{and} \quad f(1,1) = 1$$

Also $f(0,1) \neq f(1,0)$.

f	0	1
0	0	0
1	1	1

or

f	0	1
0	0	1
1	0	1

i.e., only the projections

Example: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

- What endomorphisms does it have? (Only id)

- Does $\mathbf{K}_{2,\leq}$ have any 2-ary polymorphisms? If $f(x,y)$ is one:

$$f(0,0) \neq f(1,1) \quad \text{and} \quad f(0,0) \leq f(1,1)$$

$$\implies \quad f(0,0) = 0 \quad \text{and} \quad f(1,1) = 1$$

Also $f(0,1) \neq f(1,0)$.

f	0	1
0	0	0
1	1	1

or

f	0	1
0	0	1
1	0	1

i.e., only the projections

- Any "interesting" 3-ary polymorphisms?

Example: $\mathbf{K}_{2,\leq} = (\{0,1\}, \neq, \leq)$.

- What endomorphisms does it have? (Only id)
- Does $\mathbf{K}_{2,\leq}$ have any 2-ary polymorphisms? If $f(x,y)$ is one:

$$f(0,0) \neq f(1,1) \quad \text{and} \quad f(0,0) \leq f(1,1)$$

$$\implies \quad f(0,0) = 0 \quad \text{and} \quad f(1,1) = 1$$

Also $f(0,1) \neq f(1,0)$.

f	0	1
0	0	0
1	1	1

or

f	0	1
0	0	1
1	0	1

i.e., only the projections

- Any "interesting" 3-ary polymorphisms? Yes!!

$$\text{majority}(x,y,z).$$

On the other hand, $\mathbf{M}_{3SAT} = (\{0,1\}, R_{3SAT})$ where

$$R_{3SAT} = \{(x_1,\ldots,x_6) : (x_1,x_2,x_3) \neq (x_4,x_5,x_6)\}$$

has only "trivial" polymorphisms (of all arities):

projections composed with an automorphism.

The same is true of $\mathbf{K}_3 = (\{0,1,2\}, \neq)$.

The algebra of a finite structure

A map $f : M^n \to M$ is **idempotent** if it satisfies $f(a, \ldots, a) = a \;\; \forall\, a \in M$.

The algebra of a finite structure

A map $f : M^n \to M$ is **idempotent** if it satisfies $f(a, \ldots, a) = a \ \ \forall a \in M$.

Definition

Given a structure $\mathbf{M}$, the **idempotent polymorphism algebra** of $\mathbf{M}$ is

$$\mathbb{M} := (M, \{\text{all idempotent polymorphisms of } \mathbf{M}\}).$$

The algebra of a finite structure

A map $f : M^n \to M$ is **idempotent** if it satisfies $f(a, \dots, a) = a \ \ \forall\, a \in M$.

Definition

Given a structure **M**, the **idempotent polymorphism algebra** of **M** is

$$\mathbb{M} := (M, \{\text{all idempotent polymorphisms of } \mathbf{M}\}).$$

M for the structure; $\mathbb{M}$ for its associated algebra.

Example:

$$\mathbf{M} = (\{0,1\}, \leq)$$
$$\mathbb{M} = (\{0,1\}, \{\text{all nonconstant monotone boolean functions}\}).$$

Fix **M**. $\mathbb{M}$ its idempotent polymorphism algebra.

Each basic relation (say k-ary) of **M**:

- is preserved (coordinate-wise) by all operations of $\mathbb{M}$ ...
- ...so is a **subuniverse** of $\mathbb{M}^k$.

Same is true for pp-definable relations of **M**.

Fix **M**. $\mathbb{M}$ its idempotent polymorphism algebra.

Each basic relation (say k-ary) of **M**:

- is preserved (coordinate-wise) by all operations of $\mathbb{M}$ ...
- ...so is a **subuniverse** of $\mathbb{M}^k$.

Same is true for pp-definable relations of **M**.

In fact:

Classical Fact (Geiger 1968, Bodnarčuk-Kalužnin-Kotov-Romov 1969)

$$\{\text{relations pp-definable in } \mathbf{M}\} = \{\text{subuniverses of powers of } \mathbb{M}\}$$

Fix **M**. $\mathbb{M}$ its idempotent polymorphism algebra.

Each basic relation (say k-ary) of **M**:

- is preserved (coordinate-wise) by all operations of $\mathbb{M}$ . . .
- . . . so is a **subuniverse** of $\mathbb{M}^k$.

Same is true for pp-definable relations of **M**.

In fact:

Classical Fact (Geiger 1968, Bodnarčuk-Kalužnin-Kotov-Romov 1969)

$$\{\text{relations pp-definable in } \mathbf{M}\} = \{\text{subuniverses of powers of } \mathbb{M}\}$$

Consequence: every pp-definable set R of **M** inherits the structure of an **algebra** $\mathbb{R}$ (in the same signature as $\mathbb{M}$).

Fix **M**. $\mathbb{M}$ its idempotent polymorphism algebra.

Each basic relation (say k-ary) of **M**:

- is preserved (coordinate-wise) by all operations of $\mathbb{M}$ ...
- ...so is a **subuniverse** of $\mathbb{M}^k$.

Same is true for pp-definable relations of **M**.

In fact:

Classical Fact (Geiger 1968, Bodnarčuk-Kalužnin-Kotov-Romov 1969)

$$\{\text{relations pp-definable in } \mathbf{M}\} = \{\textbf{subalgebras} \text{ of powers of } \mathbb{M}\} = \mathsf{SP}(\mathbb{M}).$$

Consequence: every pp-definable set R of **M** inherits the structure of an **algebra** $\mathbb{R}$ (in the same signature as $\mathbb{M}$).

Dictionary

structure	algebra
base **M**	associated $\mathbb{M}$
pp-def. relation R	algebra $\mathbb{R} \in \mathsf{SP}(\mathbb{M})$
pp-def. equivalence relation on R	congruence of $\mathbb{R}$
pp-def. quotient R/E	quotient algebra $\mathbb{R}/E \in \mathsf{HSP}(\mathbb{M})$
pp-def. function	homomorphism
pp-interp. structure (N, R) (R: k-ary)	$\mathbb{N} \in \mathsf{HSP}(\mathbb{M})$ with $\mathbb{R} \le \mathbb{N}^k$
$\mathbf{M}_{3SAT} \overset{pp}{\not\leadsto} \mathbf{M}$	?

Theorem 1 (Taylor '77 + Hobby-McKenzie '88 + Bulatov-Jeavons-Krokhin '05 + Maróti-McKenzie '08 + Siggers '10 + Barto-Kozik '12)

M a finite structure, $\mathbb{M}$ its idempotent polymorphism algebra. TFAE:

1. $\mathbf{M}_{3SAT} \overset{pp}{\not\rightsquigarrow} \mathbf{M}$.

Theorem 1 (Taylor '77 + Hobby-McKenzie '88 + Bulatov-Jeavons-Krokhin '05 + Maróti-McKenzie '08 + Siggers '10 + Barto-Kozik '12)

M a finite structure, $\mathbb{M}$ its idempotent polymorphism algebra. TFAE:

1. $\mathbf{M}_{3SAT} \overset{pp}{\not\to} \mathbf{M}$.
2. $\neg\exists\, \mathbb{N} \in \mathsf{HSP}(\mathbb{M})$ with $N = \{0,1\}$ and $R_{3SAT} \leq \mathbb{N}^6$ (all ops of $\mathbb{N}$ are proj's).

Theorem 1 (Taylor '77 + Hobby-McKenzie '88 + Bulatov-Jeavons-Krokhin '05 + Maróti-McKenzie '08 + Siggers '10 + Barto-Kozik '12)

M a finite structure, $\mathbb{M}$ its idempotent polymorphism algebra. TFAE:

1. $\mathbf{M}_{3SAT} \overset{pp}{\not\to} \mathbf{M}$.
2. $\neg\exists\, \mathbb{N} \in \mathsf{HSP}(\mathbb{M})$ with $N = \{0,1\}$ and $R_{3SAT} \leq \mathbb{N}^6$ (all ops of $\mathbb{N}$ are proj's).
3. $\mathbb{M}$ has an "interesting" (*Taylor*) operation[1].

[1] An operation f satisfying a system Σ of one or more identities, each of the form $f(\text{variables}) = f(\text{variables})$, nontrivial in that Σ can't be modeled by $f =$ projection on $\{0,1\}$.

Theorem 1 (Taylor '77 + Hobby-McKenzie '88 + Bulatov-Jeavons-Krokhin '05 + Maróti-McKenzie '08 + Siggers '10 + Barto-Kozik '12)

M a finite structure, $\mathbb{M}$ its idempotent polymorphism algebra. TFAE:

1. $\mathbf{M}_{3SAT} \overset{pp}{\not\to} \mathbf{M}$.
2. $\neg\exists\, \mathbb{N} \in \mathsf{HSP}(\mathbb{M})$ with $N = \{0,1\}$ and $R_{3SAT} \leq \mathbb{N}^6$ (all ops of $\mathbb{N}$ are proj's).
3. $\mathbb{M}$ has an "interesting" (*Taylor*) operation[1].
4. For some $n > 1$, $\mathbb{M}$ has a *cyclic* operation $c(x_1,\ldots,x_n)$, i.e.,
$$c(x_1,x_2,\ldots,x_n) = c(x_2,\ldots,x_n,x_1) \quad \forall x_1,\ldots,x_n \in M.$$
5. $\mathbb{M}$ has a *Siggers* operation $s(x_1,\ldots,x_6)$, i.e., satisfying
$$s(x,x,y,y,z,z) = s(y,z,z,x,x,y) \quad \forall x,y,z \in M.$$

[1] An operation f satisfying a system Σ of one or more identities, each of the form $f(\text{variables}) = f(\text{variables})$, nontrivial in that Σ can't be modeled by $f =$ projection on $\{0,1\}$.

(1) $\mathbf{M}_{3SAT} \stackrel{pp}{\not\to} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x,x,y,y,z,z) = s(y,z,z,x,x,y).$$

Proof sketch of (1) $\iff$ (5) (Siggers).

($\Longleftarrow$)

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x, x, y, y, z, z) = s(y, z, z, x, x, y).$$

Proof sketch of (1) $\iff$ (5) (Siggers).

($\Longleftarrow$) Assume $\mathbb{M}$ has such an operation $s(x_1 \ldots, x_6)$.

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x, x, y, y, z, z) = s(y, z, z, x, x, y).$$

Proof sketch of (1) $\iff$ (5) (Siggers).

($\Longleftarrow$) Assume $\mathbb{M}$ has such an operation $s(x_1 \ldots, x_6)$.

Let $\mathbf{N} = \mathbf{M}_{3SAT} = (\{0, 1\}, R_{3SAT})$.

Assume $\mathbf{N} \overset{pp}{\hookrightarrow} \mathbf{M}$.

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x, x, y, y, z, z) = s(y, z, z, x, x, y).$$

Proof sketch of (1) $\iff$ (5) (Siggers).

($\Longleftarrow$) Assume $\mathbb{M}$ has such an operation $s(x_1 \ldots, x_6)$.

Let $\mathbf{N} = \mathbf{M}_{3SAT} = (\{0, 1\},\ R_{3SAT})$.

Assume $\mathbf{N} \overset{pp}{\hookrightarrow} \mathbf{M}$.

Then $N = \{0, 1\}$ expands to $\mathbb{N} \in \mathrm{HSP}(\mathbb{M})$ with $R_{3SAT} \leq \mathbb{N}^6$.

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x,x,y,y,z,z) = s(y,z,z,x,x,y).$$

Proof sketch of (1) $\iff$ (5) (Siggers).

($\Longleftarrow$) Assume $\mathbb{M}$ has such an operation $s(x_1 \ldots, x_6)$.

Let $\mathbf{N} = \mathbf{M}_{3SAT} = (\{0,1\},\ R_{3SAT})$.

Assume $\mathbf{N} \overset{pp}{\hookrightarrow} \mathbf{M}$.

Then $N = \{0,1\}$ expands to $\mathbb{N} \in \mathrm{HSP}(\mathbb{M})$ with $R_{3SAT} \leq \mathbb{N}^6$.

On the one hand, every operation of $\mathbb{N}$ is a projection.

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x,x,y,y,z,z) = s(y,z,z,x,x,y).$$

Proof sketch of (1) $\iff$ (5) (Siggers).

($\Longleftarrow$) Assume $\mathbb{M}$ has such an operation $s(x_1 \ldots, x_6)$.

Let $\mathbf{N} = \mathbf{M}_{3SAT} = (\{0,1\},\ R_{3SAT})$.

Assume $\mathbf{N} \overset{pp}{\hookrightarrow} \mathbf{M}$.

Then $N = \{0,1\}$ expands to $\mathbb{N} \in \mathrm{HSP}(\mathbb{M})$ with $R_{3SAT} \leq \mathbb{N}^6$.

On the one hand, every operation of $\mathbb{N}$ is a projection.

On the other hand, $\mathbb{N}$ has the operation $s^{\mathbb{N}}$.

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x, x, y, y, z, z) = s(y, z, z, x, x, y).$$

Proof sketch of (1) $\iff$ (5) (Siggers).

($\Longleftarrow$) Assume $\mathbb{M}$ has such an operation $s(x_1 \ldots, x_6)$.

Let $\mathbf{N} = \mathbf{M}_{3SAT} = (\{0, 1\},\ R_{3SAT})$.

Assume $\mathbf{N} \overset{pp}{\hookrightarrow} \mathbf{M}$.

Then $N = \{0, 1\}$ expands to $\mathbb{N} \in \mathsf{HSP}(\mathbb{M})$ with $R_{3SAT} \leq \mathbb{N}^6$.

On the one hand, every operation of $\mathbb{N}$ is a projection.

On the other hand, $\mathbb{N}$ has the operation $s^{\mathbb{N}}$.

$s^{\mathbb{N}}$ satisfies the identity in (5), so cannot be a projection.

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x,x,y,y,z,z) = s(y,z,z,x,x,y).$$

$(\implies)$

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x, x, y, y, z, z) = s(y, z, z, x, x, y).$$

($\Longrightarrow$) Assume (1).

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x, x, y, y, z, z) = s(y, z, z, x, x, y).$$

($\Longrightarrow$) Assume (1).

Let $\mathbb{F}$ be the free algebra for HSP($\mathbb{M}$) on free generators x, y, z.
($\mathbb{F}$ is finite, $\mathbb{F} \in$ HSP($\mathbb{M}$).)

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\hookrightarrow} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x,x,y,y,z,z) = s(y,z,z,x,x,y).$$

($\Longrightarrow$) Assume (1).

Let $\mathbb{F}$ be the free algebra for HSP($\mathbb{M}$) on free generators x, y, z. ($\mathbb{F}$ is finite, $\mathbb{F} \in$ HSP($\mathbb{M}$).)

Let E be the subuniverse of $\mathbb{F}^2$ generated by

$$\binom{x}{y}, \binom{x}{z}, \binom{y}{z}, \binom{y}{x}, \binom{z}{x}, \binom{z}{y}.$$

Symmetry of the generators $\Longrightarrow$ E is symmetric (as a relation).

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\rightarrow} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1,\ldots,x_6)$ satisfying

$$s(x,x,y,y,z,z) = s(y,z,z,x,x,y).$$

$(\implies)$ Assume (1).

Let $\mathbb{F}$ be the free algebra for HSP($\mathbb{M}$) on free generators x, y, z. ($\mathbb{F}$ is finite, $\mathbb{F} \in$ HSP($\mathbb{M}$).)

Let E be the subuniverse of $\mathbb{F}^2$ generated by

$$\binom{x}{y}, \binom{x}{z}, \binom{y}{z}, \binom{y}{x}, \binom{z}{x}, \binom{z}{y}.$$

Symmetry of the generators $\implies$ E is symmetric (as a relation).

Let $\mathbf{G} = (F, E)$ (a structure, one binary relation).

(1) $\mathbf{M}_{3SAT} \overset{pp}{\not\to} \mathbf{M}$.

(5) $\mathbb{M}$ has an operation $s(x_1, \ldots, x_6)$ satisfying

$$s(x, x, y, y, z, z) = s(y, z, z, x, x, y).$$

($\Longrightarrow$) Assume (1).

Let $\mathbb{F}$ be the free algebra for HSP($\mathbb{M}$) on free generators x, y, z. ($\mathbb{F}$ is finite, $\mathbb{F} \in$ HSP($\mathbb{M}$).)

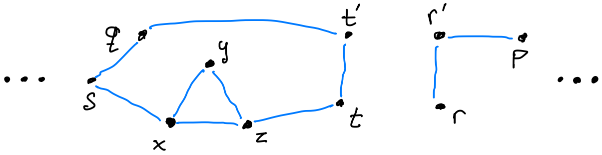
Let E be the subuniverse of $\mathbb{F}^2$ generated by

$$\binom{x}{y}, \binom{x}{z}, \binom{y}{z}, \binom{y}{x}, \binom{z}{x}, \binom{z}{y}.$$

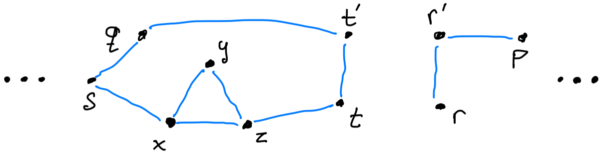
Symmetry of the generators $\Longrightarrow$ E is symmetric (as a relation).

Let $\mathbf{G} = (F, E)$ (a structure, one binary relation).

Observe: $\mathbb{F} \in$ HSP($\mathbb{M}$), $E \leq \mathbb{F}^2$ $\Longrightarrow$ $\mathbf{G} \overset{pp}{\hookrightarrow} \mathbf{M}$.

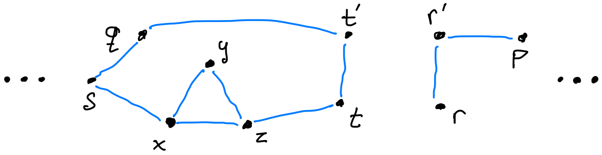


$\mathbf{G} = (F, E)$



$\mathbf{G} = (F, E)$

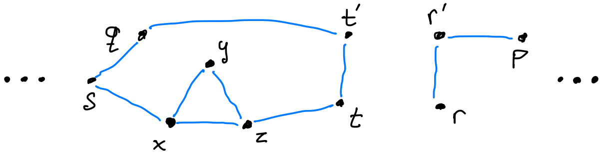
Case 1: E is irreflexive, i.e., $(p, p) \notin E$ for all $p \in F$.



$\mathbf{G} = (F, E)$

Case 1: E is irreflexive, i.e., $(p, p) \notin E$ for all $p \in F$.

Then $\mathbf{G}$ is a (simple) graph, and non-bipartite.



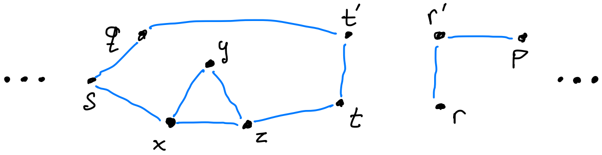
$$\mathbf{G} = (F, E)$$

Case 1: E is irreflexive, i.e., $(p,p) \notin E$ for all $p \in F$.

Then $\mathbf{G}$ is a (simple) graph, and non-bipartite.

Thus (Bulatov 2005, building on Hell-Nešetřil 1990):

$$\mathbf{K}_3 \overset{pp}{\hookrightarrow} \mathbf{G}.$$



$$\mathbf{G} = (F, E)$$

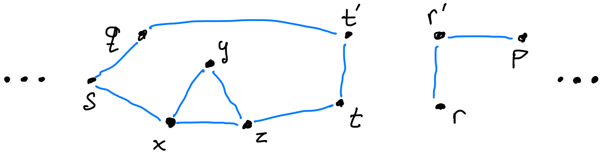
Case 1: E is irreflexive, i.e., $(p, p) \notin E$ for all $p \in F$.

Then $\mathbf{G}$ is a (simple) graph, and non-bipartite.

Thus (Bulatov 2005, building on Hell-Nešetřil 1990):

$$\mathbf{K}_3 \xhookrightarrow{pp} \mathbf{G}.$$

Known: $\mathbf{M}_{3SAT} \xhookrightarrow{pp} \mathbf{K}_3.$



$$\mathbf{G} = (F, E)$$

Case 1: E is irreflexive, i.e., $(p, p) \notin E$ for all $p \in F$.

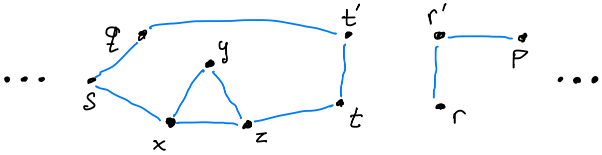
Then $\mathbf{G}$ is a (simple) graph, and non-bipartite.

Thus (Bulatov 2005, building on Hell-Nešetřil 1990):

$$\mathbf{K}_3 \overset{pp}{\hookrightarrow} \mathbf{G}.$$

Known: $\mathbf{M}_{3SAT} \overset{pp}{\hookrightarrow} \mathbf{K}_3$.

By construction, $\mathbf{G} \overset{pp}{\hookrightarrow} \mathbf{M}$.



$$\mathbf{G} = (F, E)$$

Case 1: E is irreflexive, i.e., $(p, p) \notin E$ for all $p \in F$.

Then $\mathbf{G}$ is a (simple) graph, and non-bipartite.

Thus (Bulatov 2005, building on Hell-Nešetřil 1990):

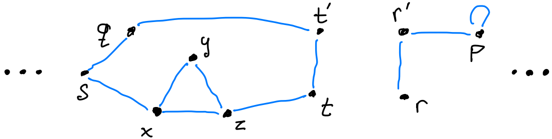
$$\mathbf{K}_3 \overset{pp}{\hookrightarrow} \mathbf{G}.$$

Known: $\mathbf{M}_{3SAT} \overset{pp}{\hookrightarrow} \mathbf{K}_3$.

By construction, $\mathbf{G} \overset{pp}{\hookrightarrow} \mathbf{M}$.

$\therefore\ \mathbf{M}_{3SAT} \overset{pp}{\hookrightarrow} \mathbf{M}$, contrary to assumption (1).

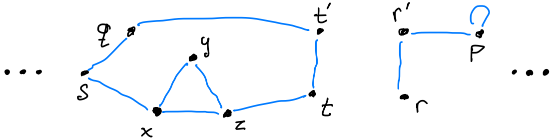
So Case 1 is impossible: there exists a loop $(p, p) \in E$.



$\mathbf{G} = (F, E)$

1

So Case 1 is impossible: there exists a loop $(p, p) \in E$.

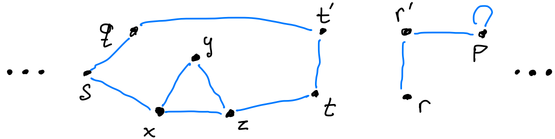


$$\mathbf{G} = (F, E)$$

Recall: E is generated by $\binom{x}{y}, \binom{x}{z}, \binom{y}{z}, \binom{y}{x}, \binom{z}{x}, \binom{z}{y}$.

1

So Case 1 is impossible: there exists a loop $(p, p) \in E$.



$\mathbf{G} = (F, E)$

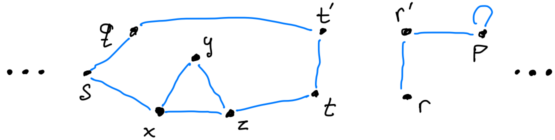
Recall: E is generated by $\binom{x}{y}, \binom{x}{z}, \binom{y}{z}, \binom{y}{x}, \binom{z}{x}, \binom{z}{y}$.

$\implies \exists$ 6-ary term[1] $s(x_1, \ldots, x_6)$ such that

$$\binom{p}{p} = s^{\mathbb{F}^2}\left(\binom{x}{y}, \binom{x}{z}, \binom{y}{z}, \binom{y}{x}, \binom{z}{x}, \binom{z}{y}\right).$$

[1] In the signature of $\mathbb{M}$, hence equal mod HSP($\mathbb{M}$) to an operation of $\mathbb{M}$.

So Case 1 is impossible: there exists a loop $(p, p) \in E$.



$\mathbf{G} = (F, E)$

Recall: E is generated by $\binom{x}{y}, \binom{x}{z}, \binom{y}{z}, \binom{y}{x}, \binom{z}{x}, \binom{z}{y}$.

$\implies \exists$ 6-ary term[1] $s(x_1, \dots, x_6)$ such that

$$\binom{p}{p} = s^{\mathbb{F}^2}\left(\binom{x}{y}, \binom{x}{z}, \binom{y}{z}, \binom{y}{x}, \binom{z}{x}, \binom{z}{y}\right).$$

A standard argument gives $\mathbb{M} \models s(x, x, y, y, z, z) = s(y, z, z, x, x, y)$. □

[1] In the signature of $\mathbb{M}$, hence equal mod HSP($\mathbb{M}$) to an operation of $\mathbb{M}$.

Summary of Lecture 1

$\mathrm{CSP}_p(\mathbf{M})$: decision problem about satisfiability of $\wedge$at-fmlas/$\mathbf{M}$.

CSP Dichotomy Theorem of Bulatov and Zhuk (2017, 2020):

$$\mathbf{M}_{3SAT} \overset{pp}{\not\to} \mathbf{M} \implies \mathrm{CSP}_p(\mathbf{M}) \text{ is in P.}$$

Algebraic perspective

- $\mathbf{M} \mapsto$ idempotent polymorphism algebra $\mathbb{M}$.
- Connections between $\mathrm{HSP}(\mathbb{M})$ and pp-definable relations over $\mathbf{M}$.

Positive characterization of $\mathbf{M}_{3SAT} \overset{pp}{\not\to} \mathbf{M}$ (Theorem 1):

"$\mathbb{M}$ has a Taylor operation"