Mal'tsev terms & compact representations

6th CWC
26.09.24 – Calfosch

Michael Kompatscher
Charles University

Local consistency: only small, local and necessary changes, does not waste resources $\Rightarrow$ *conservative*

Linear equations: costly, ineffective (Gaussian elimination), constantly invents something new that never works out (more effective algorithms) $\Rightarrow$ *socialist*

Fun fact: Finite-domain CSP solved by a combination of local consistency and linear equations (Bulatov, Zhuk, 2017)

Tomáš Nagy
AAA105
„Neoliberalism and local consistency"

Mal'tsev terms, compact representations & socialism

6th CWC
26.09.24 - Calfosch

Michael Kompatscher
Charles University

The dialectical materialism of linear equations

Example: solving linear equations over $\mathbb{Z}_3$

- row echolon form $\rightsquigarrow$ basis of solution space

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 \end{pmatrix} \bar{x} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \iff \bar{x} \in V := \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \left\langle \begin{pmatrix} -1 \\ -2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

- adding an equation $\rightsquigarrow$ intersecting spaces

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \bar{x} = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} \iff \bar{x} \in V \cap W \qquad W = \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

- Gauss elimination $\rightsquigarrow$ find basis of intersection

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} \bar{x} = \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix} \iff \bar{x} \in V \cap W = \begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \end{pmatrix} + \left\langle \begin{pmatrix} -1 \\ -1 \\ -2 \\ 1 \end{pmatrix} \right\rangle$$

The dialectical materialism of linear equations

Example: solving linear equations over $\mathbb{Z}_3 \cong \mathrm{CSP}(\mathbb{Z}_3^{rel})$

$$\mathbb{Z}_3^{rel} := (\mathbb{Z}_3, \{0\}, \{1\}, \{2\}, R_+) \quad R_+ = \{(x,y,z) \mid z \equiv x+y \ (3)\}$$

solve $R_+(x_1, x_2, x_4) \wedge (x_2 = 2) \wedge R_+(x_4, x_4, x_3) \wedge \dots$

by iteratively computing canonical generating sets of solution set of first n constraints.

(closure under $x-y+z$)

How far can this idea be pushed?

BD '06 : Mal'tsev
D '05 : maj.-min.
IMMVW '10 : few subpowers

Outline

1) What are Mal'tsev constraints?

2) What are the „canonical generating sets"?
compact representations

3) The algorithm

4) Beyond CSP

Bulatov, Dalmau

2006 A simple algorithm for Mal'tsev constraints

Mal'tsev operation

$d: A^3 \to A$ is <u>Mal'tsev</u>
if $d(yxx) \approx d(xxy) \approx y$

Mal'cev
Malcev
Maltsev
Мальцев

An algebra $\underline{A}$ / clone $\mathcal{C}$ is <u>Mal'tsev</u> if $Clo(\underline{A})$ / $\mathcal{C}$ contains a Mal'tsev operation.

Examples

- ring $(A; +, 0, -, \cdot)$ $\qquad d(xyz) = x - y + z$
- group $(A; \cdot, 1, ^{-1})$ $\qquad d(xyz) = x \cdot y^{-1} z$
- BA $(A, \wedge, \vee, 0, 1, \neg)$ $\qquad d(xyz) = (x \wedge y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (\neg x \wedge \neg y \wedge z)$
- minority $\qquad m(xyy) \approx m(yxy) = m(xyy) = x$
- semilattice $(A, \wedge)$ $\qquad$ ✗

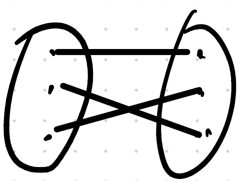
Mal'tsev operation

$d: A^3 \to A$ is Mal'tsev

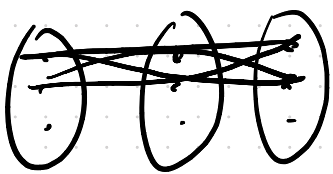
if $d(yxx) \approx d(xxy) \approx y$

Examples (polymorphisms)

- $\mathbb{Z}_3^{rel} \rightsquigarrow x - y + z \in Pol(\mathbb{Z}_3^{rel})$ [A^{rel} for every ab group]
- $A = (\{0,1,2\}, (\pi)_{\pi \in S_3}, R_{01})$ $R_{01} = \{(xyz) \in \{0,1\}^3 \mid x+y \equiv z \ (2)\}$



$\pi = (2,3)$



R

$$d(xyz) = \begin{cases} \cancel{x}\, y & \text{if } |\{x\,y\,z\}| = 3 \\ m(xyz) & \text{else} \end{cases}$$

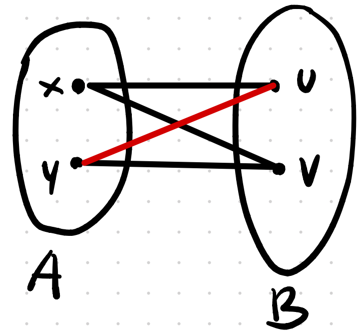
$\in Pol(A)$

The parallelogram property

$R \subseteq A \times B$ has the parallelogram property (▱)

iff $\begin{cases} (x,u) \in R \\ (x,v) \in R \\ (y\ v) \in R \end{cases}$

$\Rightarrow (y,u) \in R$

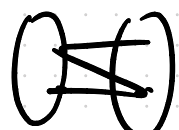


$R \subseteq A_1 \times A_2 \times \dots \times A_n$ has (▱) iff $R \subseteq \prod_{i \in I} A_i \times \prod_{i \notin I} A_j$ has (▱) $\forall I \subseteq [n]$

Ex.

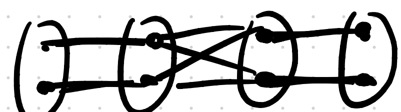
(▱)

$x_1 \leq x_2$



not (▱)

$x_1 + x_2 + x_3 + x_4 = 0$



(▱)

The parallelogram property

$R \leq \mathbb{A}^n$, $\mathbb{A}$ Mal'tsev $\Rightarrow$ R has (▱)

$$\begin{pmatrix} x \\ u \end{pmatrix}, \begin{pmatrix} x \\ v \end{pmatrix}, \begin{pmatrix} y \\ v \end{pmatrix} \in R \Rightarrow \begin{pmatrix} d(x\,x\,y) \\ d(u\,v\,v) \end{pmatrix} = \begin{pmatrix} y \\ u \end{pmatrix} \in R$$

Theorem (Mal'tsev '54)
For finite $\mathbb{A}$: $\mathbb{A}$ Mal'tsev $\Leftrightarrow$ $\forall R \leq \mathbb{A}^n$ R has (▱)

Proof ($\Leftarrow$)

$$\mathrm{Clo}^3(\mathbb{A}) = \mathrm{Sg}(\underset{x}{\pi_1^1}, \underset{y}{\pi_1^2}, \underset{z}{\pi_1^3}) \leq \mathbb{A}^{A^3}$$

$$R = \mathrm{Sg}\left(\begin{pmatrix} y \\ x \end{pmatrix}, \begin{pmatrix} x \\ x \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix}\right) \leq (\mathbb{A}^{A^3})^2 \text{ has (▱)} \Rightarrow \begin{pmatrix} y \\ y \end{pmatrix} \in R$$

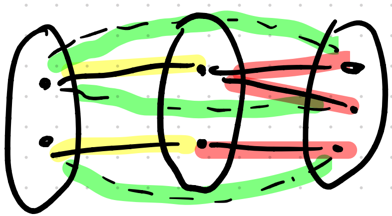
$$\Rightarrow \exists d \in \mathrm{Clo}(\mathbb{A}) : \begin{pmatrix} y \\ y \end{pmatrix} = d\begin{pmatrix} y & x & x \\ x & x & y \end{pmatrix} \quad \square$$

The parallelogram property

Theorem (Mal'tsev '54)
For finite $\underline{A}$: $\underline{A}$ Mal'tsev $\Leftrightarrow$ $\forall R \leq \underline{A}^n$ R has $(\square)$

If $\alpha, \beta \in \mathrm{Con}(\underline{A})$

$\gamma = \alpha \circ \beta \leq \underline{A}^2$, reflexive



γ has $(\square) \Rightarrow \gamma \in \mathrm{Con}(\underline{A})$

Ex.: $\underline{G}$ group $N, M \trianglelefteq G \Rightarrow NM = MN \trianglelefteq \underline{G}$

Original formulation

$\mathcal{V} = HSP(\underline{A})$ has Mal'tsev term

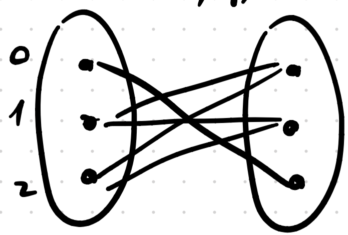
$\Leftrightarrow$

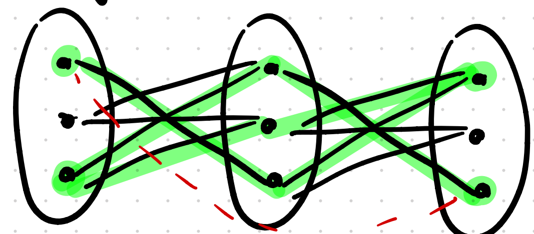
$\forall \underline{B} \in \mathcal{V}, \forall \alpha, \beta \in \mathrm{Con}(\underline{B})$:
$\alpha \circ \beta = \beta \circ \alpha = \alpha \vee \beta$

The parallelogram property

Theorem (Mal'tsev '54)
For finite $\underline{A}$: $\underline{A}$ Mal'tsev $\Leftrightarrow \forall R \leq \underline{A}^n$ R has (▱)

Remark: $R(x,y)$ $\qquad Q(x,y) = \exists z\, R(x,z) \wedge R(z,y)$





$(0,0) \in Q$
$(2,0) \in Q$
$(2,2) \in Q$
$(0,2) \notin Q$

has (▱) $\qquad$ has no (▱)

$(\{0,1,2\}, R)$ has no Mal'tsev polymorphism!

Question: How hard is checking if $\mathrm{Pol}(\mathbb{A})$ is Mal'tsev?

Outline

1) What are Mal'tsev constraints? ✓

2) What are the „canonical generating sets"?
compact representations

3) The algorithm

4) Beyond CSP

Bulatov, Dalmau

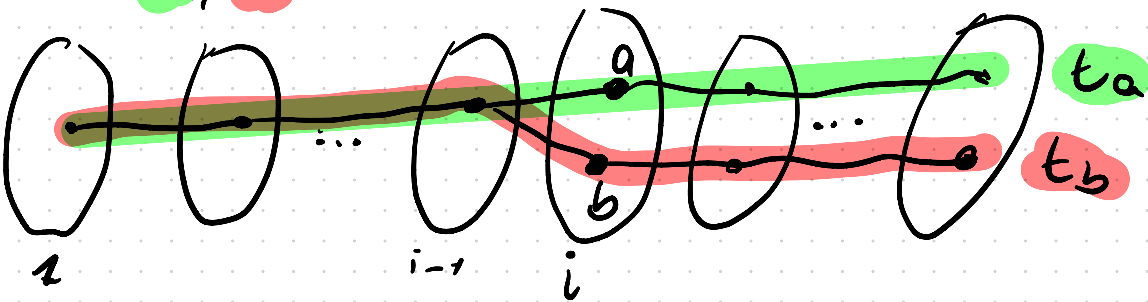
2006 A simple algorithm for Mal'tsev constraints

Forks and Signatures

$R \subseteq A^n$

Def. $(i, a, b) \in [n] \times A^2$ is a <u>fork of R</u>

$\exists\ t_a, t_b \in R$:

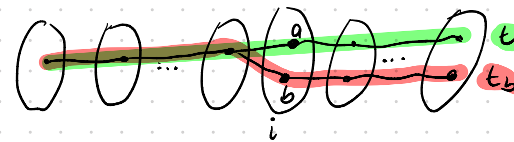


<u>Signature of R</u> $= Sig(R) = \{(i,a,b) \mid (i,a,b) \text{ fork of } R\}$

<u>Ex.</u> $Sig\left(\underset{x+y=z}{R^+}\right) = \{1,2\} \times \mathbb{Z}_3^2 \cup \{3\} \times (=) \quad = Sig\left(\{(xyz)\} \mid y = z\right)$

Forks and Signatures

$$\mathrm{Sig}(R) = \{ (i,a,b) \mid (i,a,b) \text{ fork of } R \}$$



Thm. $\mathbf{A}$ Mal'tsev, $\mathbf{R} \leq \mathbf{A}^n$, $C \subseteq R$ s.t. $\mathrm{Sig}(C) = \mathrm{Sig}(\mathbf{R})$ $\Rightarrow$ $\mathrm{Sg}_{\mathbf{A}^n}(C) = \mathbf{R}$

Proof: Induction on n. $n = 1 \Rightarrow C = R$ ✓

$n-1 \to n$: Let $\begin{pmatrix} \bar{a} \\ b \end{pmatrix} \in R$. $\stackrel{IH}{\Longrightarrow} \exists \begin{pmatrix} \bar{a} \\ c \end{pmatrix} \in \mathrm{Sg}(C) \subseteq R$

$\Rightarrow (n,b,c) \in \mathrm{Sig}(R) = \mathrm{Sig}(C) \Rightarrow \exists$ witnesses $\begin{pmatrix} \bar{t} \\ b \end{pmatrix}, \begin{pmatrix} \bar{t} \\ c \end{pmatrix} \in C$

$$d\left(\begin{pmatrix} \bar{a} \\ c \end{pmatrix}, \begin{pmatrix} \bar{t} \\ c \end{pmatrix}, \begin{pmatrix} \bar{t} \\ b \end{pmatrix} \right) = \begin{pmatrix} \bar{a} \\ b \end{pmatrix} \in \mathrm{Sg}(C)$$

$\square$

Compact Representations

Thm. $\underline{A}$ Mal'tsev, $\underline{R} \leq \underline{A}^n$, $C \subseteq \underline{R}$ s.t. $Sig(C) = Sig(\underline{R})$ $\Rightarrow$ $Sg_{\underline{A}^n}(C) = \underline{R}$

Def. For $R \leq \underline{A}^n$, $C \subseteq R$ is a compact representation (CR)

$$:\Leftrightarrow \begin{cases} \cdot)\ Sig(C) = Sig(R) \\ \cdot)\ |C| \leq 2 \cdot Sig(C) \leq 2n|A|^2 \end{cases}$$

by the proof

if $\bar{a} \in R \Rightarrow \exists\, \bar{c}_i, \bar{d}_i \in C$

$$\bar{a} = d(\cdots d(d(\bar{c}_1, \underbrace{\bar{d}_2, \bar{c}_2}_{2\text{-fork}}), \underbrace{\bar{d}_3, \bar{c}_3}_{3\text{-fork}}) \cdots \underbrace{\bar{d}_n, \bar{c}_n}_{n\text{-fork}})$$

Compact Representations

$\Rightarrow$ Given CR C of $R \leq \underline{A}^n$

$\bar{a} \in R$? is decidable in time $\mathcal{O}(n^2)$.

1) $\exists\, \bar{c}_1 \in C : c_1[1] = a[1]$?

   if NO $\rightarrow$ return NO

2) for $i = 2, 3, \dots n$

   $\exists\, \bar{d}_i, \bar{c}_i \in C$ witnessing the i-fork

   $(d(\cdot d(c_1, d_2, c_2) \cdots d_{i-1}, c_{i-1})[i], a[i])$

   if NO $\rightarrow$ return NO

3) return YES $(\bar{a} = d(\cdots d(\bar{c}_1, \bar{d}_2, \bar{c}_2), \dots \bar{d}_n, \bar{c}_n))$

Compact Representations

Example

•) affine basis for $R = \begin{pmatrix}1\\0\\1\\1\end{pmatrix} + \left\langle \begin{pmatrix}1\\0\\0\\2\end{pmatrix}, \begin{pmatrix}0\\1\\1\\1\end{pmatrix} \right\rangle \leq \mathbb{Z}_3^4$

$C = \left\{ \begin{pmatrix}1\\0\\1\\1\end{pmatrix} + i \begin{pmatrix}1\\0\\0\\2\end{pmatrix}, \begin{pmatrix}1\\0\\1\\1\end{pmatrix} + j \cdot \begin{pmatrix}0\\1\\1\\1\end{pmatrix} \;\middle|\; i, j \in \mathbb{Z}_3 \right\}$ is a CR of R.

•) For a group $\underline{G}$, $H \leq \underline{G}^n$

„strong generating sets" of $\underline{H}$ $\rightsquigarrow$ compact representation of $H \leq \underline{G}^n$

(Schreier-Sims ~70ies)

Outline

1) What are Mal'tsev constraints? ✓

2) What are the „canonical generating sets"?
   compact representations ✓

3) The algorithm

4) Beyond CSP

Bulatov, Dalmau

2006 A simple algorithm for Mal'tsev constraints

The algorithm for Mal'tsev CSPs

$\mathbb{A} = (A; R_1, \dots, R_n)$ $\quad d(x,y,z) \in \mathrm{Pol}(\mathbb{A})$ Mal'tsev

$\underline{A} := (A, d(x,y,z))$

recall: want to solve $\mathrm{CSP}(\mathbb{A})$

$$\exists \bar{x} : R_{i_1}(\quad \dots \quad) \wedge R_{i_2}(\quad \dots \quad) \wedge \dots \wedge R_{i_k}(\quad \dots \quad)$$

CR

by iteratively computing compact representations, solving:

Intersect($\underline{A}$)

Input: CR's C_1, C_2 of $R_i = S_g(C_i) \leq \underline{A}^n$

Output: CR of $R_1 \cap R_2$
(or $\emptyset$ if $R_1 \cap R_2 = \emptyset$)

The algorithm for Mal'tsev CSPs [Zeb's CSP notes]

Algorithm 4 `Nonempty`$(R, i_1, ..., i_k, \mathbb{S})$, p a Mal'cev term, R a compact representation of $\mathbb{R} \leq \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$, $\mathbb{S} \leq \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$.

poly$(|R|, |A|^k)$

```
Set R' ← R.
while π_{i_1,...,i_k}(R') is not closed under p and R' ∩ S = ∅ do
    Pick t_1, t_2, t_3 ∈ R' with π_{i_1,...,i_k}(p(t_1, t_2, t_3)) ∉ π_{i_1,...,i_k}(R').
    Set R' ← R' ∪ {p(t_1, t_2, t_3)}.
if R' ∩ S ≠ ∅ then
    return any element of R' ∩ S.
else
    return ∅.
```

exhaustively compute $R' = \pi_{i_1,\dots,i_k}(\mathbb{R})$

return $\bar{a} \in R \cap \mathbb{S}$ or $\emptyset$

The algorithm for Mal'tsev CSPs [Zeb's CSP notes]

Algorithm 4 $\texttt{Nonempty}(R, i_1, \ldots, i_k, \mathbb{S})$, p a Mal'cev term, R a compact representation of $\mathbb{R} \leq \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$, $\mathbb{S} \leq \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$.

$\mathrm{poly}(|R|, |A|^k)$

$\rightsquigarrow \bar{a} \in R \cap S$ or $\emptyset$

Algorithm 5 $\texttt{Fix-values}(R, a_1, \ldots, a_m)$, p a Mal'cev term, R a compact representation of $\mathbb{R} \leq \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$.

```
Set R_0 ← R.
for j from 1 to m do
    if (j, a_j, a_j) ∉ Sig(R_{j-1}) then
        return ∅.
    else
        Set R_j ← {t}, where t ∈ R_{j-1} and the pair t,t witnesses the triple (j, a_j, a_j).
    for all (i, a, b) ∈ Sig(R_{j-1}) with i > j do
        Let t_a, t_b ∈ R_{j-1} witness the triple (i, a, b).
        Let t ← Nonempty(R_{j-1}, j, i, {(a_j, a)}).
        if t ≠ ∅ then
            Set R_j ← R_j ∪ {t, p(t, t_a, t_b)}.
return R_m.
```

$R_j \ldots$ CR of $R \wedge (x_1 = a_1) \wedge \ldots \wedge (x_j = a_j)$

$t, p(t, t_a, t_b)$ witnesses

$t[i] = a \quad p(t, t_a, t_b)[i] = p(aab) = b$

The algorithm for Mal'tsev CSPs [Zeb's CSP notes]

Algorithm 4 `Nonempty`$(R, i_1, \dots, i_k, \mathbb{S})$, p a Mal'cev term, R a compact representation of $\mathbb{R} \leq \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$, $\mathbb{S} \leq \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$.

poly$(|R|, |A|^k)$

$\rightsquigarrow$ $\bar{a} \in R \cap S$ or $\emptyset$

Algorithm 5 `Fix-values`$(R, a_1, \dots, a_m)$, p a Mal'cev term, R a compact representation of $\mathbb{R} \leq \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$.

poly$(|R|, m)$

$\rightsquigarrow$ CR of $\mathbb{R} \wedge x_1 = a_1, \dots$ or $\emptyset$

Algorithm 6 `Next-beta`$(R, i_1, \dots, i_k, \mathbb{S})$, R a compact representation of $\mathbb{R} \leq \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$, $\mathbb{S} \leq \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$.

Set $R' \leftarrow \emptyset$.
for all $(i, a, b) \in \mathrm{Sig}(R)$ **do**
  Set $t_a \leftarrow$ `Nonempty`$(R, i_1, \dots, i_k, i, \mathbb{S} \times \{a\})$.
  if $t_a \neq \emptyset$ **then**
    Set $t_b \leftarrow$ `Nonempty`(`Fix-values`$(R, \pi_1(t_a), \dots, \pi_{i-1}(t_a)), i_1, \dots, i_k, i, \mathbb{S} \times \{b\})$.
    if $t_b \neq \emptyset$ **then**
      Set $R' \leftarrow R' \cup \{t_a, t_b\}$.
return R'.

poly$(|R|, |A|^k)$

$\rightsquigarrow$ CR of $R \cap S$ or $\emptyset$

witnesses for forks of $R \cap S$

The algorithm for Mal'tsev CSPs [Zeb's CSP notes]

Algorithm 4 `Nonempty`$(R, i_1, ..., i_k, \mathbb{S})$, p a Mal'cev term, R a compact representation of $\mathbb{R} \le \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$, $\mathbb{S} \le \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$.

$\text{poly}(|R|, |A|^k)$

$\rightsquigarrow \bar{a} \in R \cap S$ or $\emptyset$

Algorithm 5 `Fix-values`$(R, a_1, ..., a_m)$, p a Mal'cev term, R a compact representation of $\mathbb{R} \le \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$.

$\text{poly}(|R|, m)$

$\rightsquigarrow$ CR of $\mathbb{R} \wedge x_1 = a_1, \ldots$ or $\emptyset$

Algorithm 6 `Next-beta`$(R, i_1, ..., i_k, \mathbb{S})$, R a compact representation of $\mathbb{R} \le \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$, $\mathbb{S} \le \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$.

$\text{poly}(|R|, |A|^k)$

$\rightsquigarrow$ CR of $R \cap S$ or $\emptyset$

Algorithm 7 `Intersect`$(R, i_1, ..., i_k, S)$, R a compact representation of $\mathbb{R} \le \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$, S a compact representation of $\mathbb{S} \le \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$.

1: Let $t_R \in R$ and $t_S \in S$ be any tuples.
2: Set $R' \leftarrow (R \times \{t_S\}) \cup (\{t_R\} \times S) \subseteq \mathbb{A}_1 \times \cdots \mathbb{A}_n \times \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$. CR of $R \times S$
3: **for** $j \le k$ **do**
4: Set $R' \leftarrow$ `Next-beta`$(R', i_j, n+j, =_{\mathbb{A}_{i_j}})$.
5: **return** a minimal subset of $\pi_{1,...,n}(R')$ which witnesses every triple $(i, a, b) \in \text{Sig}(\pi_{1,...,n}(R'))$.

The algorithm for Mal'tsev CSPs [Zeb's CSP notes]

Algorithm 4 `Nonempty`$(R, i_1, \ldots, i_k, \mathbb{S})$, p a Mal'cev term, R a compact representation of $\mathbb{R} \le \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$, $\mathbb{S} \le \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$.

poly$(|R|, |A|^k)$

$\rightsquigarrow \bar{a} \in \mathbb{R} \cap \mathbb{S}$ or $\emptyset$

Algorithm 5 `Fix-values`$(R, a_1, \ldots, a_m)$, p a Mal'cev term, R a compact representation of $\mathbb{R} \le \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$.

poly$(|R|, m)$

$\rightsquigarrow$ CR of $\mathbb{R} \wedge x_1 = a_1, \ldots$ or $\emptyset$

Algorithm 6 `Next-beta`$(R, i_1, \ldots, i_k, \mathbb{S})$, R a compact representation of $\mathbb{R} \le \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$, $\mathbb{S} \le \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$.

poly$(|R|, |A|^k)$

$\rightsquigarrow$ CR of $\mathbb{R} \cap \mathbb{S}$ or $\emptyset$

Algorithm 7 `Intersect`$(R, i_1, \ldots, i_k, S)$, R a compact representation of $\mathbb{R} \le \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$, S a compact representation of $\mathbb{S} \le \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$.

1: Let $t_R \in R$ and $t_S \in S$ be any tuples.
2: Set $R' \leftarrow (R \times \{t_S\}) \cup (\{t_R\} \times S) \subseteq \mathbb{A}_1 \times \cdots \mathbb{A}_n \times \mathbb{A}_{i_1} \times \cdots \times \mathbb{A}_{i_k}$. CR of $R \times S$
3: **for** $j \le k$ **do**
4: Set $R' \leftarrow$ `Next-beta`$(R', i_j, n+j, =_{\mathbb{A}_{i_j}})$.
5: **return** a minimal subset of $\pi_{1,\ldots,n}(R')$ which witnesses every triple $(i, a, b) \in \operatorname{Sig}(\pi_{1,\ldots,n}(R'))$.

poly$(|R|, |S|)$

$\rightsquigarrow$ CR of $\mathbb{R} \wedge \mathbb{S}$ or $\emptyset$.

$\Rightarrow$ $\boxed{\mathrm{CSP}(\mathbb{A}) \in \mathrm{P}}$ for $\mathrm{Pol}(\mathbb{A})$ Mal'tsev

Outline

1) What are Mal'tsev constraints? ✓

2) What are the „canonical generating sets"?
   compact representations ✓

3) The algorithm ✓ *

4) Beyond CSP

Bulatov, Dalmau

2006 A simple algorithm for Mal'tsev constraints

Is the algorithm necessary? ("in the light of CLAP")

Yes!

→ Monday

(next... my slide before Mo...)

Is the algorithm necessary? ("in the light of CLAP")

$\mathbb{A}$ Mal'tsev $\quad d(yxy) = d(yxx) = d(xxy) = y$

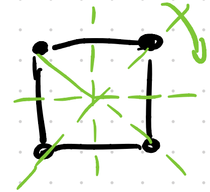
- CSP($\mathbb{A}$) has bounded width $\Leftrightarrow$ Pol($\mathbb{A}$) has majority
- If $x-y+z \in \mathrm{Pol}(\mathbb{A}) \to$ alt. terms $x_1 - x_2 + x_3 - x_4 \ldots + x_n \in \mathrm{Pol}(\mathbb{A})$

  $\Rightarrow$ CSP($\mathbb{A}$) solvable by AIP
- $\mathbb{A} = (\{0,1,2\}, (\pi)_{\pi \in S_3}, R_{01}) \xrightarrow{AT}$ CSP($\mathbb{A}$) solved by AIP.
- Pol($\mathbb{A}$) conservative $\rightsquigarrow$ Andrew's talk! $\oplus L - \varepsilon$

> [BGWŽ '20]
>
> PCSP($\mathbb{A},\mathbb{B}$) is solvable by BLP+AIP
>
> $\Leftrightarrow$ Pol($\mathbb{A},\mathbb{B}$) has block symmetric t
>
> $$t(\overleftrightarrow{x_1 \ldots x_\ell}, \overleftrightarrow{x_{\ell+1}, \ldots x_{2\ell+1}}) \quad \forall \ell \geq 1$$

An example not solved by BLP+AIP

$(D_8, \cdot)$ dihedral group ....



$t \in Clo(D_8, \cdot)$

$[x,y] = x^{-1}y^{-1}xy$

has normal form

$$t(x_1 \dots x_n) = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots x_n^{\alpha_n} [x_1,x_2]^{\beta_{12}} [x_1,x_3]^{\beta_{13}} \cdot \dots \cdot [x_{n-1},x_n]^{\beta_{n-1,n}}$$

$\alpha_i \in [4]$
$\beta_{ij} \in [2]$

Claim: $\nexists$ idempotent blocksymmetric $t \in Clo(D_8, \cdot)$

Pf. Assume $t(x_1 \dots x_n) = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \dots x_n^{\alpha_n} [x_1,x_2]^{\beta_{12}} [x_1,x_3]^{\beta_{13}} \cdot \dots \cdot [x_{n-1},x_n]^{\beta_{n-1,n}}$ is block symmetric $t(\overleftrightarrow{x_1 \dots x_{\frac{n}{2}}}\ \overleftrightarrow{x_{\frac{n}{2}+1} \dots x_n})$, idempotent

(i) $x = t(xx \dots \dots x) = x^{\sum_i \alpha_i} \Rightarrow \exists \alpha_i = \pm 1$ (wlog $i=1$)

(ii) $t(x1, \dots\dots 1) = t(1x1 \dots 1) \Rightarrow \alpha_1 = \alpha_2 = \alpha$

(iii) $t(xy1 \dots 1) = x^\alpha y^\alpha [x,y]^{\beta_{12}}$
$\shortparallel$
$t(yx1 \dots 1) = y^\alpha x^\alpha [y,x]^{\beta_{12}}$

$[x,y] = [y,x]$

$\Rightarrow x \cdot y = y \cdot x$ in D_8 ↯

An example not solved by BLP+AIP

Thm. $\boxed{\begin{array}{l}\text{[AMM'14] For every finite Mal'tsev } \underline{A}, \\ \exists\, \mathbb{A} = (A, R_1, \dots, R_n) : \mathrm{Pol}(\mathbb{A}) = \mathrm{Clo}(\underline{A})\end{array}}$

$\Rightarrow \exists\ \mathbb{D} = (D_8, R_1, \dots, R_n) : \mathrm{Pol}(\mathbb{D}) = \mathrm{Clo}(D_8, xy^{-1}z)$

CSP($\mathbb{D}$) solved by Mal'tsev, not AIP+BLP.

Moreover $\mathrm{Clo}(D_8, xy^{-1}z)$ is minimal Taylor.

→ Is CSP($\mathbb{D}$) solved by CLAP?

[AMM'14] uses compactness.

⇝ How can we construct $\mathbb{A}$ from $\underline{A}$?

Mal'tsev terms, relational bases

& socialism

6th CWC
27.09.24 – Calfosch

Michael Kompatscher
Charles University

... Yesterday

Thm. [AMM'14] For every finite Mal'tsev $\underline{A}$,
$\exists\, \mathbb{A} = (A, R_1, \dots, R_n)$ $\mathrm{Pol}(\mathbb{A}) = \mathrm{Clo}(\underline{A})$

$R \leq S \leq \underline{A}^n$

$\mathrm{Sig}(R) \subsetneq \mathrm{Sig}(S)$

(non-constr. proof)

·) $\forall n$: $\mathrm{Clo}(\underline{A})^n \leq A^{A^n}$ has forks $(\bar{a}, f(\bar{a}), g(\bar{a}))$

·) $\lambda((c,d)) := \{\bar{a} \in A^{<\omega} \mid (\bar{a}, c, d)$ not fork$\}$ $\xrightarrow{\text{compactness}}$ $\exists$ fin. many „minimal" $\bar{a}$ in $\lambda(c,d)$

·) take $m := \max|\bar{a}|$ $\Rightarrow$ $\mathrm{Clo}(\underline{A}) = \mathrm{Pol}(\mathrm{Clo}(\underline{A})^m)$

Question today: How can we construct $\mathbb{A} = (A, \underbrace{R_1, \dots, R_n}_{\text{relational basis}})$?

↳ In general unknown, e.g. for $(G, xy^{-1}z)$

Motivation 1

Thm. [AMM '14] For every finite Mal'tsev $\underline{A}$, $\exists \mathbb{A} = (A, R)$ $\quad Pol(\mathbb{A}) = Clo(\underline{A})$

Cor.: For fixed $\underline{A}$ Mal'tsev Term($\underline{A}$) is in P

Input: $f : A^n \to A$

Question: Is $f \in Clo(\underline{A})$?

check if f preserves R

cannot describe algorithm, unless we know R

Remark

$\exists \underline{A}$: Term($\underline{A}$) $\in$ EXPTIME-c. [Kozik '08]

fin. not Mal'tsev

Motivation 2

Thm. [AMM'14] For every finite Mal'tsev $\underline{A}$,
$\exists \mathbb{A} = (A, R)$ $\quad \mathrm{Pol}(\mathbb{A}) = \mathrm{Clo}(\underline{A})$

Corollary:
On fixed A $\exists \leq$ coutable Mal'tsev clones

Can we classify them?

$\iff$ Can we classify Mal'tsev CSP templates up to pp-definability?

Motivation 2

Thm [Bulatov '05] $Clo(\underline{A}) = Pol(Inv^{(4)}(\underline{A}))$

On $|A| = 3$, there are 1129 Mal'tsev clones.

Why?

But on $|A| = 4$

$$\underline{A}_k := (\mathbb{Z}_4, +, 0, -, 2x_1 \cdot x_2 \cdot \ldots \cdot x_k)$$

$$Clo(\underline{A}_n) = \{ \sum \alpha_i x_i + 2 \cdot p(x_1 \ldots x_n) \mid deg(p) \leq k \}$$

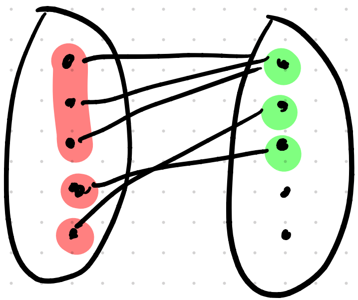
$$Clo(\underline{A}_1) \subsetneq Clo(\underline{A}_2) \subsetneq Clo(\underline{A}_3) \subsetneq \ldots$$

Basic questions are still open, e.g:

$\exists$ infinite antichain on some A?

An observation

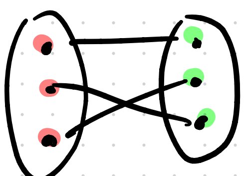
$\underline{A}$ Mal'tsev, $R \leq \underline{A}^2$



$(x,y) \mapsto (x/\alpha_1, y/\alpha_2)$

maps to

$\bar{R}$



$\underline{A}_1 = pr_1 R/\alpha_1 \qquad \underline{A}_2 = pr_2 R/\alpha_2$

Link-congruences $\alpha_i \in \mathrm{Con}(pr_i R)$

$x \,\alpha_1\, y :\Leftrightarrow \exists z\, R(x\,z) \wedge R(y\,z)$

$x \,\alpha_2\, y \Leftrightarrow \exists z\, R(z\,x) \wedge R(z\,y)$

- So binary relations $R \leq \underline{A}^2 \leftrightarrow$ isomorphisms $\bar{R} \leq \underline{A}_1 \times \underline{A}_2$ $\quad \underline{A}_i \in HS(\underline{A})$
- Similarly $R \leq \underline{A}^n \leftrightarrow$ reduced representation $\bar{R} \leq_{sd} \underline{A}_1 \times \dots \times \underline{A}_n \quad \underline{A}_i \in HS(\underline{A})$

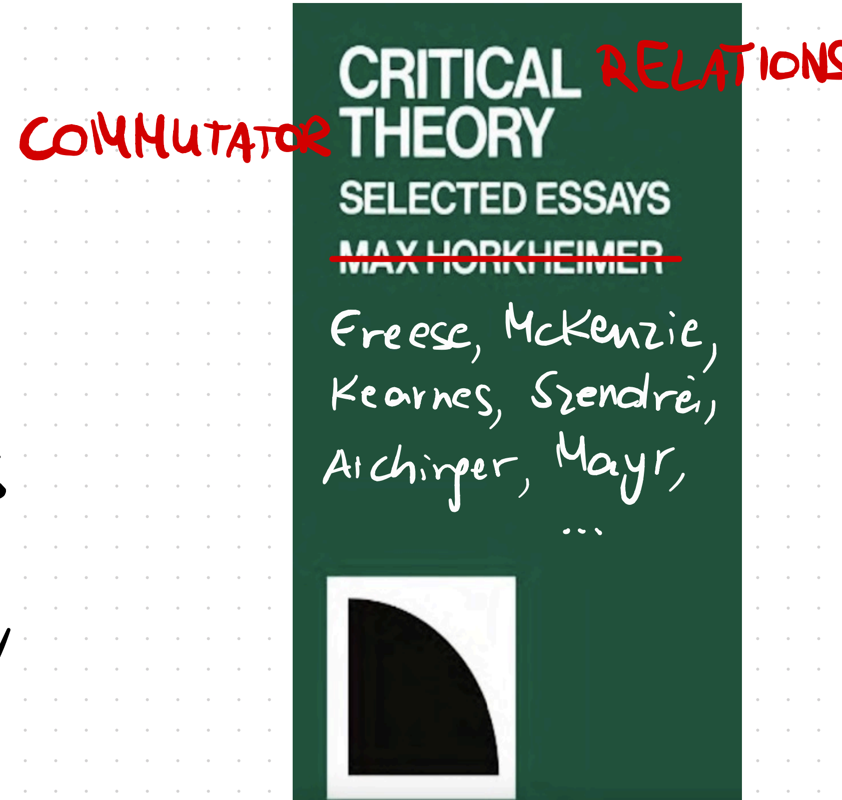
Outline

1) Relational basis ✓

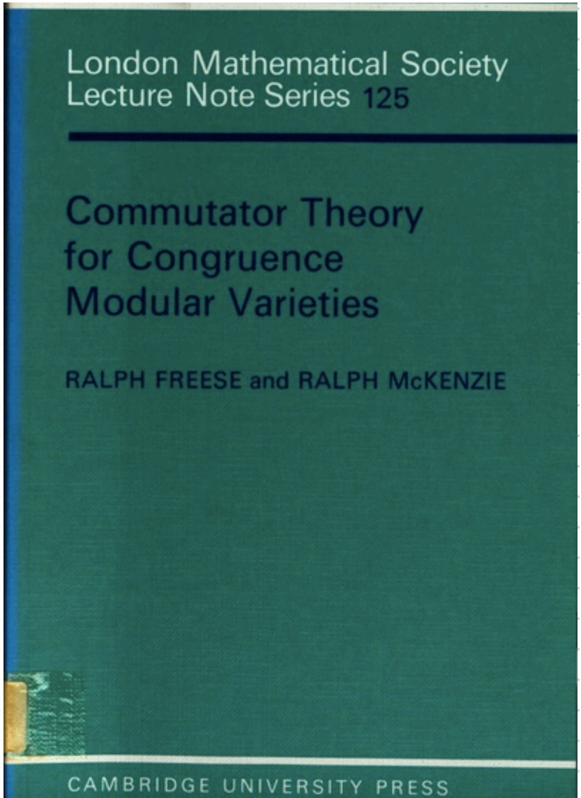
2) Commutator theory

3) Critical relations

4) 3-element Mal'tsev algebras



Commutator Theory



Generalizes concepts as

Abelian
nilpotent
solvable

commutator
centralizer
...

groups / NS
↓ ↓
algebras / congruences.

Abelianness

$\underline{A}$ … algebra with Mal'tsev term $d(x\,y\,z)$

Def. $\boxed{\underline{A} \text{ is } \textbf{Abelian} \;:\Longleftrightarrow\; d = \left\{ \begin{matrix} x & - & d(x\,y\,z) \\ | & & | \\ y & - & z \end{matrix} \;\middle|\; x, y, z \in A \right\} \leq \underline{A}^4}$

Ex. $\underline{G} = (G, \cdot, 1, {}^{-1})$ group, $d(x\,y\,z) = x y^{-1} z$

$\underline{G}$ Abelian $\qquad d \leq \underline{G}^4$

$$\begin{matrix} 1 & - & a \\ | & & | \\ 1 & - & a \end{matrix} \;,\; \begin{matrix} b & - & b \\ | & & | \\ 1 & - & 1 \end{matrix} \in d \Rightarrow \begin{matrix} b & - & ab \\ | & & | \\ 1 & - & a \end{matrix} \in d \Rightarrow ab = b \cdot 1^{-1} a = ba$$

$\rightarrow \underline{G}$ abelian

Thm [S. ~70ies] $\underline{A}$ Abelian $\Longleftrightarrow$ $\mathrm{Clo}(\underline{A}, (a)_{a \in A}) = \left\{ \bar{x} \mapsto \sum_{i=1}^{n} r_i \cdot x_i + c \right\}$ w.r.t. a module

Centralizers

Def. $\alpha \in \mathrm{Con}(\underline{G})$ Abelian $:\Longleftrightarrow$ $\qquad d(xyz)$

$$d\Gamma_\alpha := \left\{ \begin{pmatrix} x & d(x,y,z) \\ y & z \end{pmatrix} \;\middle|\; x\,\alpha\, y\,\alpha\, z \right\} \leq \underline{A}^4 \qquad x = d(xyy)$$

α centralizes β $:\Longleftrightarrow$

$$d\Gamma_{\alpha,\beta} := \left\{ \begin{pmatrix} x & d(xyz) \\ y & z \end{pmatrix} \;\middle|\; x\,\alpha\, y\,\beta\, z \right\} \leq \underline{A}^4$$

centralizer $(0_A : \alpha)$ $:\Longleftrightarrow$ biggest β : $d\Gamma_{\alpha,\beta} \leq \underline{A}^4$

Ex. In groups $\underline{G}$ $\quad \alpha \in \mathrm{Con}(\underline{G}) \leftrightsquigarrow N \trianglelefteq G \quad x\alpha y \Leftrightarrow xy^{-1} \in N$

α centralizes β $\Longleftrightarrow$ for $N = [1]_\alpha$, $M = [1]_\beta$ $\quad \forall n \in N, m \in M$:

$$n \cdot m = m \cdot n$$

Central congruences

Unlike in groups for $\underline{A}$ Maltsev, $\alpha \in \mathrm{Con}(\underline{A})$

$|[a]_\alpha| \neq |[b]_\alpha|$ possible.

<u>But</u> if α centralizes $1_A = A \times A$ ("α is central")

$$\left\{ \begin{matrix} x & - & d(x,y,z) \\ | & & | \\ y & - & z \end{matrix} \right\} = d\Gamma_{\alpha,1} = Sg_{\underline{A}^4}\left\{ \begin{matrix} x & - & y \\ | & & | \\ x & - & y \end{matrix} , \begin{matrix} u & - & u \\ | & & | \\ v & - & v \end{matrix} \right\} = \left\{ \begin{matrix} x & - & y \\ | & & | \\ d(x,y,z) & - & z \end{matrix} \right\} \leq \underline{A}^4$$

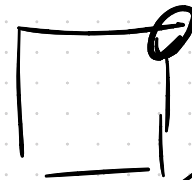
$$d\Gamma_{\alpha,1} \leq \underline{A}^4$$

$\Rightarrow$ For fixed a,b $\;x \mapsto d(x,a,b)$ is bijection from $[a]_\alpha \to [b]_\alpha$

$$\Rightarrow \boxed{|[a]_\alpha| = |[b]_\alpha| \text{ for } \alpha \text{ central.}}$$

Commutator

$$\underline{\Delta}_{\alpha\beta} = Sg_{\underline{A}^4}\left(d\!\int_{\alpha\;\beta} \right)$$



$[\alpha, \beta] :=$ linkedness-congruence

$\Leftrightarrow$ $[\alpha, \beta]$ is smallest $\gamma \in Con(\underline{A})$:

in $\underline{A}/\gamma$ α/γ centralizes β/γ

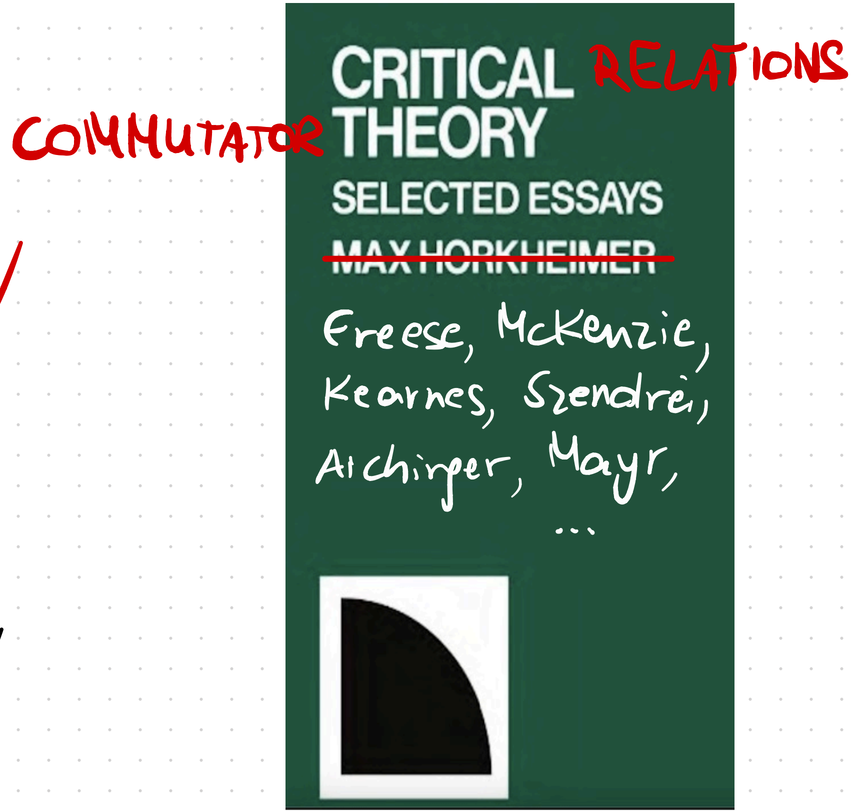
Outline

1) Relational basis ✓

2) Commutator theory ✓

3) Critical relations

4) 3-element Mal'tsev algebras



Critical relations

Def. For algebra $\underline{A}$,

$R \leq \underline{A}^n$ is critical $:\Leftrightarrow$

- $\nexists\, R < R_1, R_2 \leq \underline{A}^n$ with $R = R_1 \wedge R_2$
- no dummy variables

Ex.

- $\underline{A} = (\{0,1\}, \wedge, \vee)$ $\leq$, $\{0\}$, $\{1\}$ critical
- $\underline{A} = (\mathbb{Z}_3, x-y+z)$

  $R(x_1 \dots x_n)$ is critical $\Leftrightarrow$ $R = \{\bar{x} \mid \sum \alpha_i x_i = c\}$ for $\alpha_i \neq 0$

Γ pp-defines $\mathrm{Inv}(\underline{A})$ $\Leftrightarrow$ Γ pp-def. all critical relations

Critical relations in Mal'tsev algebras

Thm. [KS'12]

$\underline{A}$ Mal'tsev, $R \le \underline{A}^n$ critical, $n \ge 3$

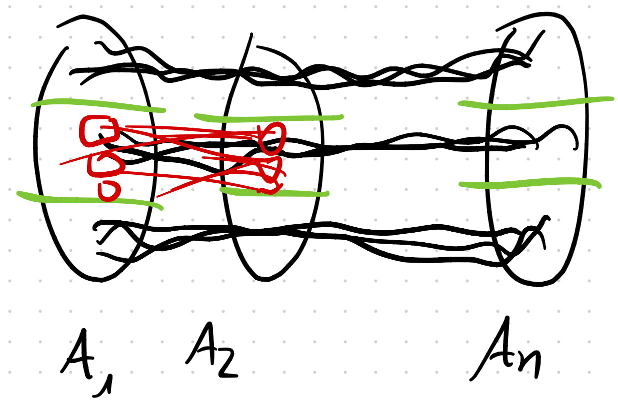
$\bar{R} \le_{sd} \underline{A}_1 \times \dots \times \underline{A}_n$ reduced rep.

$\Rightarrow$ 1) $\mathrm{Con}(\underline{A}_i) =$ 

, μ_i Abelian

2) $pr_{i,j} \bar{R}$ is isomorphism

$\underline{A}_i/(0:\mu_i) \to \underline{A}_j/(0:\mu_j)$



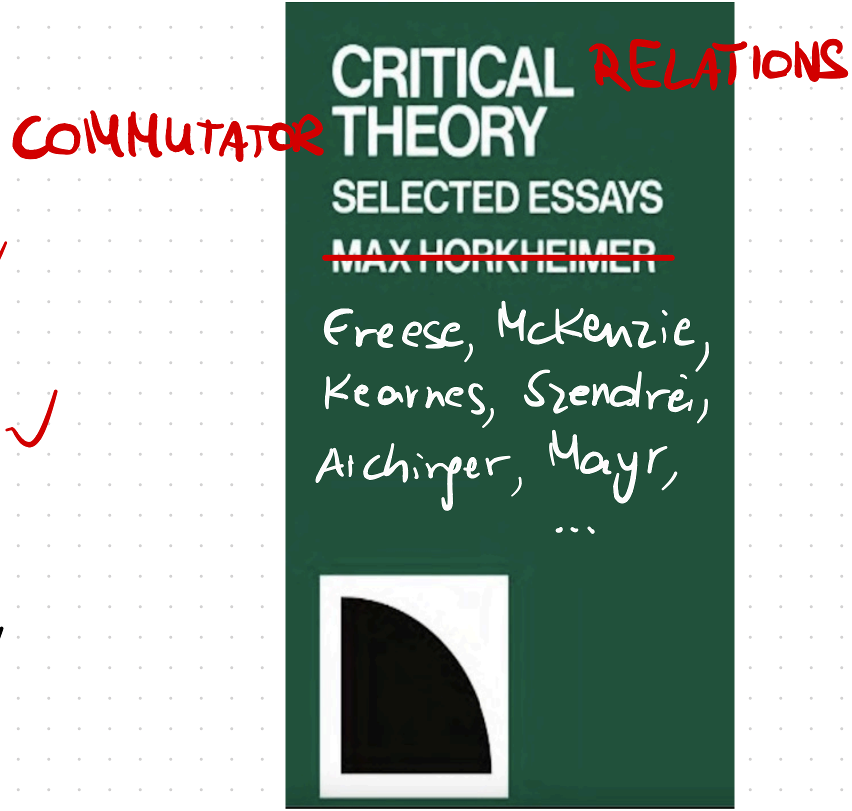
Outline

1) Relational basis ✓

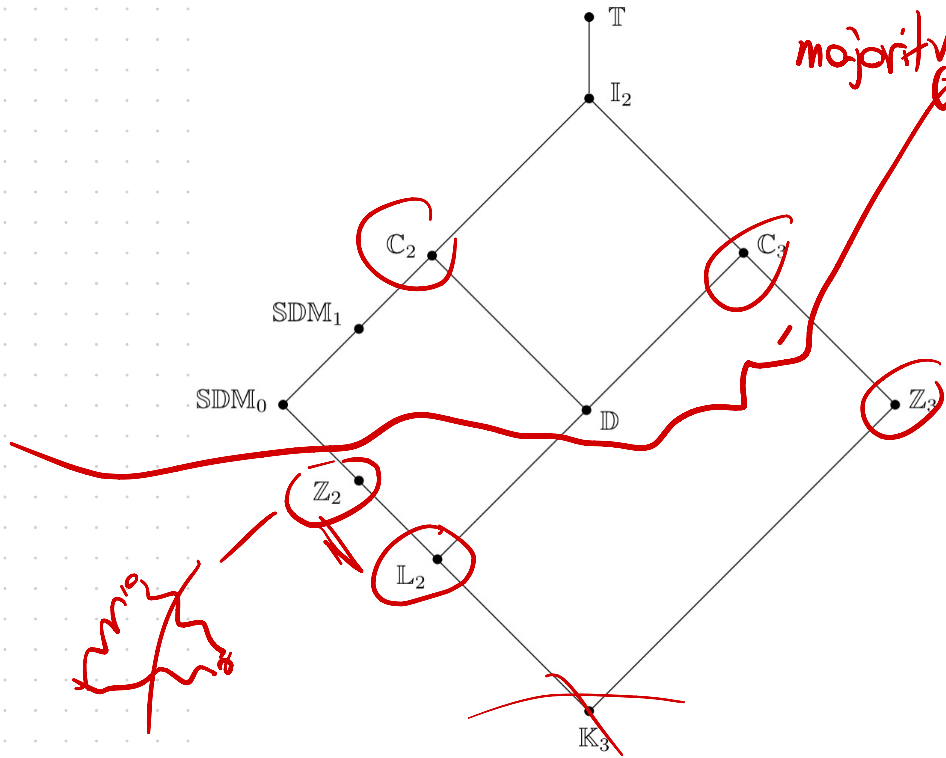
2) Commutator theory ✓

3) Critical relations ✓

4) 3-element Mal'tsev algebras



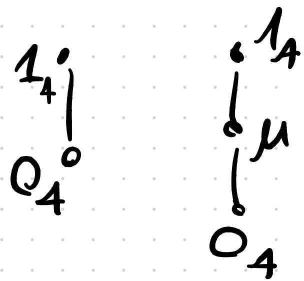
3-element Mal'tsev up to minion homom.



$\underline{A}$ Mal'tsev $\quad A = \{0,1,2\}$

$R \leq \underline{A}^2 \leftrightarrow$ isomorphisms: $HS(\underline{A})$

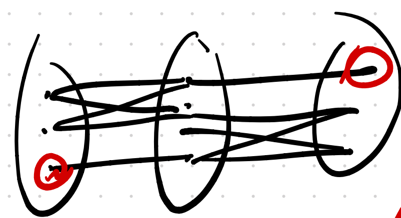
Lemma $\operatorname{Con}\underline{A}$



Proof Assume

$01|2, \; 0|12 \in \operatorname{Con}\underline{A}$

$\alpha \qquad \beta$



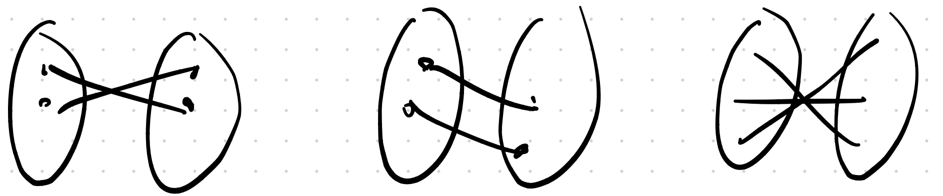
$(2,0) \notin \alpha\circ\beta$

$(0,2) \in$

$\lightning$

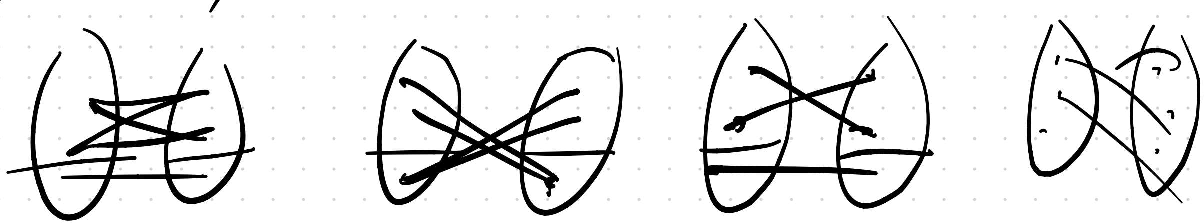
If $\underline{A}$ simple

$\to$ R is a partial isomorphism



If $\exists\, \mu \neq 0_A, 1_A$

μ



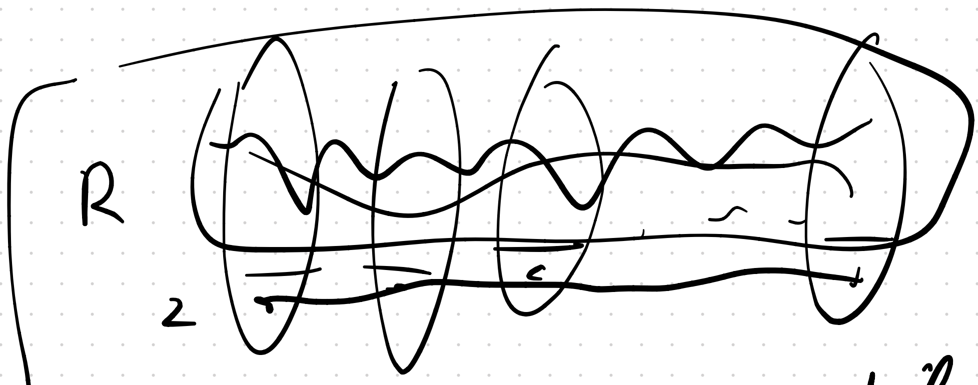
$|A|^{|A|+1} \cdot ((B(|A|+1)-1)$

$\mu = 0 1/2 \in \mathrm{Con}\,\underline{A}$

μ is not central

If μ is Abelian $\Rightarrow$ $\mu = (0:\mu)$

Def If $\forall B \in HS(\underline{A})$,
μ_B Abelian monolith of $\underline{B}$
$\Rightarrow (0:\mu_B)$ is Abelian
$\Rightarrow \underline{A}$ satisfies (C1)



$\{\sum \alpha_i x_i = c \ (2)\}$

R is pp-def by $d\int_\mu$ and binary

1) No algebra in $HS(\underline{A})$ has Ab. monolith

$\Rightarrow$ all crit. rel. have arity ≤ 2

$\Leftrightarrow$ $\underline{A}$ has majority

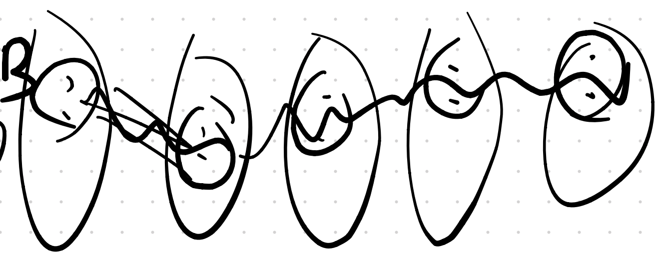
2) $R \leq \underline{A}^n$ $R = \overline{R} \leq \underline{A}_1 \times \dots \times \underline{A}_n$

assume $\underline{A}_i$ are not Abelian $\Rightarrow$ $|A_i| = 3$

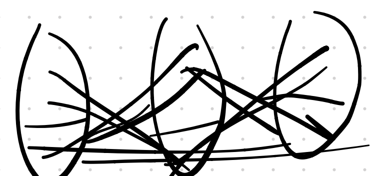
μ_i Abelian $\mu_i' = (0 : \mu_i)$

3) $\exists \underline{A}_i$ Abelian $\Rightarrow \forall \underline{A}_i$ Abelian

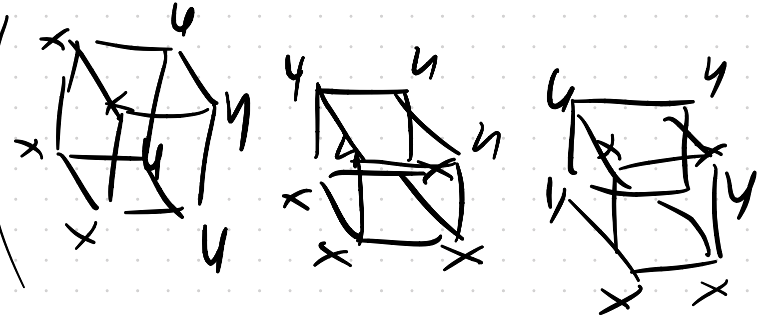
$|A_i| = 3 \to \underline{A} = \mathbb{Z}_3$

$|A_i| = 2$ B  -- pp-definable by $d\restriction_B$

if all $\underline{A}_i \in S(\underline{A})$

$\underline{A}_i \in H(A)$  -- pp-definable by $d/_{\mu}$

$[\alpha,\beta]$ -- linkedness $S_p\left(\begin{tikzcd} x \arrow[r, dash, "\beta"] \arrow[d, dash, "\alpha"'] & x \arrow[d, dash, "\alpha"] \\ y \arrow[r, dash, "\beta"'] & y \end{tikzcd} \quad \begin{tikzcd} u \arrow[r, dash, "D"] \arrow[d, dash, "\alpha"'] & v \arrow[d, dash, "\nu"] \\ u \arrow[r, dash, "\beta"'] & v \end{tikzcd}\right)$

$[1,1,1] = 0$ $S_G\Bigg($  $\Bigg) = \Delta_{111}$

linkedness in 1 coordinate

$(\mathbb{Z}_4, +, 0, -, 2xy)$ -- $\underline{\Delta_{111}}$ is critical
?

(D_8)?