Failure of local-to-global

Alexandr Kazda, **Michael Kompatscher**

University of Oxford

05/02/2021

AAA100 - Krakow

Deciding Maltsev conditions

Deciding Maltsev conditions

Definition

A (strong) Maltsev condition Σ is a set of functional equations, e.g. $f(x,x,y) \approx f(x,y,x) \approx f(x,x,y)$

$\mathbf{A}$ *satisfies* Σ, if $\mathbf{A}$ has a term $f^{\mathbf{A}}$ such that $\forall x,y \in A : f^{\mathbf{A}}(x,x,y) = f^{\mathbf{A}}(x,y,x) = f^{\mathbf{A}}(x,x,y)$.

Deciding Maltsev conditions

Definition

A (strong) Maltsev condition Σ is a set of functional equations, e.g.
$f(x,x,y) \approx f(x,y,x) \approx f(x,x,y)$

$\mathbf{A}$ *satisfies* Σ, if $\mathbf{A}$ has a term $f^{\mathbf{A}}$ such that
$\forall x,y \in A : f^{\mathbf{A}}(x,x,y) = f^{\mathbf{A}}(x,y,x) = f^{\mathbf{A}}(x,x,y)$.

For a fixed Maltsev condition Σ define the computational problem:

Decide(Σ)
INPUT: finite algebra $\mathbf{A} = (A, f_1, \ldots, f_n)$
QUESTION: Does $\mathbf{A}$ satisfy Σ?

Deciding Maltsev conditions

Why study Decide(Σ)?

Deciding Maltsev conditions

Why study Decide(Σ)?

- Meta-problem for CSPs?

Deciding Maltsev conditions

Why study Decide(Σ)?

- ~~Meta-problem for CSPs?~~ Input encoded as algebra

Deciding Maltsev conditions

Why study Decide(Σ)?

- ~~Meta-problem for CSPs?~~ Input encoded as algebra
- variant of the Subpower Membership Problem?
  test if $f(x_1, x_2, x_3) \in \mathbf{F}_{\mathbf{A}}(x_1, x_2, x_3) \leq \mathbf{A}^{\mathbf{A}^3}$

Deciding Maltsev conditions

Why study Decide(Σ)?

- ~~Meta-problem for CSPs?~~ Input encoded as algebra
- variant of the Subpower Membership Problem?
  test if $f(x_1, x_2, x_3) \in \mathbf{F}_{\mathbf{A}}(x_1, x_2, x_3) \leq \mathbf{A}^{\mathbf{A}^3}$
- testing properties of algebras
- fun with algebras / relations

Deciding Maltsev conditions

Why study Decide(Σ)?

- ~~Meta-problem for CSPs?~~ Input encoded as algebra
- variant of the Subpower Membership Problem?
  test if $f(x_1, x_2, x_3) \in \mathbf{F_A}(x_1, x_2, x_3) \leq \mathbf{A}^{\mathbf{A}^3}$
- testing properties of algebras
- fun with algebras / relations

The bad news (Freese, Valeriote '09)

In many cases Decide(Σ) is EXPTIME-complete
(semilattice, CD(n) for $n > 3$, $t(x, \ldots, x) \approx x$, CM, CD,...)

Deciding Maltsev conditions

Why study Decide(Σ)?

- ~~Meta-problem for CSPs?~~ Input encoded as algebra
- variant of the Subpower Membership Problem?
  test if $f(x_1, x_2, x_3) \in \mathbf{F}_{\mathbf{A}}(x_1, x_2, x_3) \leq \mathbf{A}^{\mathbf{A}^3}$
- testing properties of algebras
- fun with algebras / relations

The bad news (Freese, Valeriote '09)

In many cases Decide(Σ) is EXPTIME-complete
(semilattice, CD(n) for $n > 3$, $t(x, \ldots, x) \approx x$, CM, CD,...)

$\rightarrow$ **idempotent variant**

Decide$^{\text{id}}(\Sigma)$
INPUT: finite *idempotent* algebra $\mathbf{A} = (A, f_1, \ldots, f_n)$
QUESTION: Does $\mathbf{A}$ satisfy Σ?

Local-to-global

Local-to-global for $t(x, y) \approx t(y, x)$

A has *local* binary symmetric terms if

$$\forall a, b \in A \, \exists t_{a,b} \in \mathrm{Clo}(\mathbf{A}) \colon \; t_{a,b}(a, b) = t_{a,b}(b, a)$$

Local-to-global for $t(x, y) \approx t(y, x)$

A has *local* binary symmetric terms if

$$\forall a, b \in A \, \exists t_{a,b} \in \mathrm{Clo}(\mathbf{A})\colon\; t_{a,b}(a, b) = t_{a,b}(b, a)$$

$$\Leftrightarrow \forall a, b \in A \, \exists q\colon\; \begin{pmatrix} q \\ q \end{pmatrix} \in Sg_{\mathbf{A}^2} \left\{ \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} b \\ a \end{pmatrix} \right\}$$

Local-to-global for $t(x, y) \approx t(y, x)$

A has *local* binary symmetric terms if

$$\forall a, b \in A\, \exists t_{a,b} \in \mathrm{Clo}(\mathbf{A})\colon\; t_{a,b}(a, b) = t_{a,b}(b, a)$$
$$\Leftrightarrow \forall a, b \in A\, \exists q\colon\; \begin{pmatrix} q \\ q \end{pmatrix} \in Sg_{\mathbf{A}^2} \left\{ \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} b \\ a \end{pmatrix} \right\}$$

Claim

If **A** has local binary symmetric terms, then it has a (global) binary symmetric term $t(x, y) \approx t(y, x)$.

Local-to-global for $t(x, y) \approx t(y, x)$

A has *local* binary symmetric terms if

$$\forall a, b \in A \, \exists t_{a,b} \in \mathrm{Clo}(\mathbf{A})\colon\; t_{a,b}(a, b) = t_{a,b}(b, a)$$
$$\Leftrightarrow \forall a, b \in A \, \exists q\colon \begin{pmatrix} q \\ q \end{pmatrix} \in Sg_{\mathbf{A}^2} \left\{ \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} b \\ a \end{pmatrix} \right\}$$

Claim

If **A** has local binary symmetric terms, then it has a (global) binary symmetric term $t(x, y) \approx t(y, x)$.

Consequence

$\mathrm{Decide}(t(x, y) \approx t(y, x)) \in \mathrm{P}$.

Proof idea

Assume $\mathbf{A}$ has local binary symmetric terms

Let $R \leq \mathbf{A}^4$ be a relation s.t.

$$\begin{pmatrix} a \\ b \\ a' \\ b' \end{pmatrix}, \begin{pmatrix} b \\ a \\ b' \\ a' \end{pmatrix} \in R$$

Proof idea

Assume **A** has local binary symmetric terms

Let $R \leq \mathbf{A}^4$ be a relation s.t.

$$\begin{pmatrix} a \\ b \\ a' \\ b' \end{pmatrix}, \begin{pmatrix} b \\ a \\ b' \\ a' \end{pmatrix} \in R$$

Then R also contains

$$\begin{pmatrix} q \\ q \\ t(a', b') \\ t(b', a') \end{pmatrix}, \begin{pmatrix} q \\ q \\ t(b', a') \\ t(a', b') \end{pmatrix} \in R$$

Proof idea

Assume $\mathbf{A}$ has local binary symmetric terms

Let $R \leq \mathbf{A}^4$ be a relation s.t.

$$\begin{pmatrix} a \\ b \\ a' \\ b' \end{pmatrix}, \begin{pmatrix} b \\ a \\ b' \\ a' \end{pmatrix} \in R$$

Then R also contains

$$\begin{pmatrix} q \\ q \\ t(a', b') \\ t(b', a') \end{pmatrix}, \begin{pmatrix} q \\ q \\ t(b', a') \\ t(a', b') \end{pmatrix} \in R \to \begin{pmatrix} q \\ q \\ q' \\ q' \end{pmatrix} \in R$$

Proof idea

Assume **A** has local binary symmetric terms

Let $R \leq \mathbf{A}^4$ be a relation s.t.

$$\begin{pmatrix} a \\ b \\ a' \\ b' \end{pmatrix}, \begin{pmatrix} b \\ a \\ b' \\ a' \end{pmatrix} \in R$$

Then R also contains

$$\begin{pmatrix} q \\ q \\ t(a', b') \\ t(b', a') \end{pmatrix}, \begin{pmatrix} q \\ q \\ t(b', a') \\ t(a', b') \end{pmatrix} \in R \rightarrow \begin{pmatrix} q \\ q \\ q' \\ q' \end{pmatrix} \in R$$

induction over all pairs (a, b)... **A** contains a binary cyclic term.

Failure for minority

m is minority operation if

$$m(x, x, y) \approx m(x, y, x) \approx m(x, x, y) \approx y$$

Failure for minority

m is minority operation if

$$m(x,x,y) \approx m(x,y,x) \approx m(x,x,y) \approx y$$

Theorem (Kazda, Opršal, Valeriote, Zhuk '19)
For every $k \geq 2$, $\exists \mathbf{A}_k$, idempotent with $|A_k| = 4k$, s.t.

- $\mathbf{A}_k$ has local minority on subsets of size $k-1$
- $\mathbf{A}_k$ has no 'global' minority

Failure for minority

m is minority operation if

$$m(x,x,y) \approx m(x,y,x) \approx m(x,x,y) \approx y$$

Theorem (Kazda, Opršal, Valeriote, Zhuk '19)
For every $k \geq 2$, $\exists \mathbf{A}_k$, idempotent with $|A_k| = 4k$, s.t.

- $\mathbf{A}_k$ has local minority on subsets of size $k-1$
- $\mathbf{A}_k$ has no 'global' minority

Note: This does *not* prove hardness of deciding minority, and $\mathrm{Decide}^{\mathrm{id}}(\mathrm{minority}) \in \mathrm{NP}$.

Failure for minority

m is minority operation if

$$m(x,x,y) \approx m(x,y,x) \approx m(x,x,y) \approx y$$

Theorem (Kazda, Opršal, Valeriote, Zhuk '19)
For every $k \geq 2$, $\exists \mathbf{A}_k$, idempotent with $|A_k| = 4k$, s.t.

- $\mathbf{A}_k$ has local minority on subsets of size $k-1$
- $\mathbf{A}_k$ has no 'global' minority

Note: This does *not* prove hardness of deciding minority, and $\text{Decide}^{\text{id}}(\text{minority}) \in \text{NP}$.

Question

When else does local-to-global fail?

G-terms

G-terms

Definition

For $G \leq \mathrm{Sym}(n)$... permutation group

t is a G-**term*** if

$t(x_1, \ldots, x_n) \approx t(x_{\pi(1)}, \ldots, x_{\pi(n)})$ for all $\pi \in G$.

*suggestions for better names are welcome.

G-terms

Definition

For $G \leq \mathrm{Sym}(n)$... permutation group
t is a G-**term*** if
$t(x_1, \dots, x_n) \approx t(x_{\pi(1)}, \dots, x_{\pi(n)})$ for all $\pi \in G$.

- If $G = \mathrm{Sym}(n)$: symmetric terms

*suggestions for better names are welcome.

G-terms

Definition

For $G \leq \mathrm{Sym}(n)$... permutation group
t is a G-**term*** if
$t(x_1, \ldots, x_n) \approx t(x_{\pi(1)}, \ldots, x_{\pi(n)})$ for all $\pi \in G$.

- If $G = \mathrm{Sym}(n)$: symmetric terms
- If $G = \mathbb{Z}_n \leq \mathrm{Sym}(n)$: cyclic terms
  $c(x_1, \ldots, x_{n-1}, x_n) \approx c(x_2, \ldots, x_n, x_1)$

*suggestions for better names are welcome.

G-terms

Definition

For $G \leq \mathrm{Sym}(n)$... permutation group
t is a G-**term*** if
$t(x_1, \ldots, x_n) \approx t(x_{\pi(1)}, \ldots, x_{\pi(n)})$ for all $\pi \in G$.

- If $G = \mathrm{Sym}(n)$: symmetric terms
- If $G = \mathbb{Z}_n \leq \mathrm{Sym}(n)$: cyclic terms
  $c(x_1, \ldots, x_{n-1}, x_n) \approx c(x_2, \ldots, x_n, x_1)$
- If 1-generated, e.g. $G = \langle (12)(345) \rangle$: 'cyclic loop conditions'

*suggestions for better names are welcome.

G-terms

Definition

For $G \leq \mathrm{Sym}(n)$... permutation group
t is a G-**term*** if
$t(x_1, \ldots, x_n) \approx t(x_{\pi(1)}, \ldots, x_{\pi(n)})$ for all $\pi \in G$.

- If $G = \mathrm{Sym}(n)$: symmetric terms
- If $G = \mathbb{Z}_n \leq \mathrm{Sym}(n)$: cyclic terms
  $c(x_1, \ldots, x_{n-1}, x_n) \approx c(x_2, \ldots, x_n, x_1)$
- If 1-generated, e.g. $G = \langle (12)(345) \rangle$: 'cyclic loop conditions'

Question (Valeriote)

For which G do G-terms have the local-to-global property?

*suggestions for better names are welcome.

G-terms

Theorem (Kazda, MK '20)
Local-to-global **works** if...

G-terms

Theorem (Kazda, MK '20)
Local-to-global **works** if...

- G has a fixpoint (trivial Maltsev condition)

G-terms

Theorem (Kazda, MK '20)
Local-to-global **works** if...

- G has a fixpoint (trivial Maltsev condition)
- $G = \mathbb{Z}_n \leq \mathrm{Sym}(n)$: cyclic terms

G-terms

Theorem (Kazda, MK '20)
Local-to-global **works** if...

- G has a fixpoint (trivial Maltsev condition)
- $G = \mathbb{Z}_n \leq \mathrm{Sym}(n)$: cyclic terms
- $G \leq \mathrm{Sym}(|G|)$ acting on itself by left translation

G-terms

Theorem (Kazda, MK '20)
Local-to-global **works** if...

- G has a fixpoint (trivial Maltsev condition)
- $G = \mathbb{Z}_n \leq \mathrm{Sym}(n)$: cyclic terms
- $G \leq \mathrm{Sym}(|G|)$ acting on itself by left translation
- $G = \langle g \rangle$ (local on k many tuples, with $k = \#$orbits)

G-terms

Theorem (Kazda, MK '20)
Local-to-global **works** if...

- G has a fixpoint (trivial Maltsev condition)
- $G = \mathbb{Z}_n \leq \text{Sym}(n)$: cyclic terms
- $G \leq \text{Sym}(|G|)$ acting on itself by left translation
- $G = \langle g \rangle$ (local on k many tuples, with k= #orbits)
- $G = D_n$ dihedral group for *even* n

G-terms

Theorem (Kazda, MK ’20)
Local-to-global **works** if...

- G has a fixpoint (trivial Maltsev condition)
- $G = \mathbb{Z}_n \leq \text{Sym}(n)$: cyclic terms
- $G \leq \text{Sym}(|G|)$ acting on itself by left translation
- $G = \langle g \rangle$ (local on k many tuples, with $k = \#$orbits)
- $G = D_n$ dihedral group for *even n*

...even for non-idempotent $\mathbf{A}$

Theorem (Kazda, MK '20)
Local-to-global **fails** if...

G-terms

Theorem (Kazda, MK '20)
Local-to-global **fails** if...

- $G = \mathrm{Sym}(n)$ for $n \geq 3$

G-terms

Theorem (Kazda, MK '20)
Local-to-global **fails** if...

- $G = \text{Sym}(n)$ for $n \geq 3$
- $G = D_n$: dihedral group for *odd* n

Theorem (Kazda, MK '20)
Local-to-global **fails** if...

- $G = \text{Sym}(n)$ for $n \geq 3$
- $G = D_n$: dihedral group for *odd* n
- $G = A_n$: alternating group for $n \geq 3$

G-terms

Theorem (Kazda, MK '20)
Local-to-global **fails** if...

- $G = \text{Sym}(n)$ for $n \geq 3$
- $G = D_n$: dihedral group for *odd* n
- $G = A_n$: alternating group for $n \geq 3$
- $\exists g \in G$ with one fixpoint and orbits of the same size otherwise.

G-terms

Theorem (Kazda, MK '20)
Local-to-global **fails** if...

- $G = \mathrm{Sym}(n)$ for $n \geq 3$
- $G = D_n$: dihedral group for *odd* n
- $G = A_n$: alternating group for $n \geq 3$
- $\exists g \in G$ with one fixpoint and orbits of the same size otherwise.

(even in idempotent algebras)

Example

Construction for $G = \mathrm{Sym}(3)$

Let $g = (1)(23)$ and $\mathbb{Z}_2 = \langle g \rangle$.
Let T be a transversal of the orbits $g \curvearrowright \{1, 2, 3\}^3$.

Set $\mathbf{A} = (\{0, 1\} \times \{1, 2, 3\} \cup \mathbb{Z}_2; t_0, t_1)$ with t_0, t_1 ternary

Example

Construction for $G = \mathrm{Sym}(3)$

Let $g = (1)(23)$ and $\mathbb{Z}_2 = \langle g \rangle$.
Let T be a transversal of the orbits $g \curvearrowright \{1, 2, 3\}^3$.

Set $\mathbf{A} = (\{0, 1\} \times \{1, 2, 3\} \cup \mathbb{Z}_2; t_0, t_1)$ with t_0, t_1 ternary

- t_i idempotent; most tuples mapped to $\mathbb{Z}_2$

Example

Construction for $G = \mathrm{Sym}(3)$

Let $g = (1)(23)$ and $\mathbb{Z}_2 = \langle g \rangle$.
Let T be a transversal of the orbits $g \curvearrowright \{1,2,3\}^3$.

Set $\mathbf{A} = (\{0,1\} \times \{1,2,3\} \cup \mathbb{Z}_2; t_0, t_1)$ with t_0, t_1 ternary

- t_i idempotent; most tuples mapped to $\mathbb{Z}_2$
- $t_i(x_1, x_2, x_3) = x_1 + x_2 + x_3$ on $\mathbb{Z}_2$

Example

Construction for $G = \mathrm{Sym}(3)$

Let $g = (1)(23)$ and $\mathbb{Z}_2 = \langle g \rangle$.
Let T be a transversal of the orbits $g \curvearrowright \{1,2,3\}^3$.

Set $\mathbf{A} = (\{0,1\} \times \{1,2,3\} \cup \mathbb{Z}_2; t_0, t_1)$ with t_0, t_1 ternary

- t_i idempotent; most tuples mapped to $\mathbb{Z}_2$
- $t_i(x_1, x_2, x_3) = x_1 + x_2 + x_3$ on $\mathbb{Z}_2$
- t_i on $(\{i\} \times \{1,2,3\})^3$ counts how often g was applied (wrt T)

Example

Construction for $G = \mathrm{Sym}(3)$

Let $g = (1)(23)$ and $\mathbb{Z}_2 = \langle g \rangle$.
Let T be a transversal of the orbits $g \curvearrowright \{1,2,3\}^3$.

Set $\mathbf{A} = (\{0,1\} \times \{1,2,3\} \cup \mathbb{Z}_2; t_0, t_1)$ with t_0, t_1 ternary

- t_i idempotent; most tuples mapped to $\mathbb{Z}_2$
- $t_i(x_1, x_2, x_3) = x_1 + x_2 + x_3$ on $\mathbb{Z}_2$
- t_i on $(\{i\} \times \{1,2,3\})^3$ counts how often g was applied (wrt T)
- t_i on $(\{1-i\} \times \{1,2,3\})^3$ is $id \in \mathbb{Z}_2$

Example

Construction for $G = \mathrm{Sym}(3)$

Let $g = (1)(23)$ and $\mathbb{Z}_2 = \langle g \rangle$.
Let T be a transversal of the orbits $g \curvearrowright \{1,2,3\}^3$.

Set $\mathbf{A} = (\{0,1\} \times \{1,2,3\} \cup \mathbb{Z}_2; t_0, t_1)$ with t_0, t_1 ternary

- t_i idempotent; most tuples mapped to $\mathbb{Z}_2$
- $t_i(x_1, x_2, x_3) = x_1 + x_2 + x_3$ on $\mathbb{Z}_2$
- t_i on $(\{i\} \times \{1,2,3\})^3$ counts how often g was applied (wrt T)
- t_i on $(\{1-i\} \times \{1,2,3\})^3$ is $id \in \mathbb{Z}_2$
- t_i is symmetric elsewhere*

Example

Construction for $G = \mathrm{Sym}(3)$

Let $g = (1)(23)$ and $\mathbb{Z}_2 = \langle g \rangle$.
Let T be a transversal of the orbits $g \curvearrowright \{1,2,3\}^3$.

Set $\mathbf{A} = (\{0,1\} \times \{1,2,3\} \cup \mathbb{Z}_2; t_0, t_1)$ with t_0, t_1 ternary

- t_i idempotent; most tuples mapped to $\mathbb{Z}_2$
- $t_i(x_1, x_2, x_3) = x_1 + x_2 + x_3$ on $\mathbb{Z}_2$
- t_i on $(\{i\} \times \{1,2,3\})^3$ counts how often g was applied (wrt T)
- t_i on $(\{1-i\} \times \{1,2,3\})^3$ is $id \in \mathbb{Z}_2$
- t_i is symmetric elsewhere*

t_i is symmetric everywhere but $(\{i\} \times \{1,2,3\})^3$.

Example

Construction for $G = \mathrm{Sym}(3)$

Let $g = (1)(23)$ and $\mathbb{Z}_2 = \langle g \rangle$.
Let T be a transversal of the orbits $g \curvearrowright \{1,2,3\}^3$.

Set $\mathbf{A} = (\{0,1\} \times \{1,2,3\} \cup \mathbb{Z}_2; t_0, t_1)$ with t_0, t_1 ternary

- t_i idempotent; most tuples mapped to $\mathbb{Z}_2$
- $t_i(x_1, x_2, x_3) = x_1 + x_2 + x_3$ on $\mathbb{Z}_2$
- t_i on $(\{i\} \times \{1,2,3\})^3$ counts how often g was applied (wrt T)
- t_i on $(\{1-i\} \times \{1,2,3\})^3$ is $id \in \mathbb{Z}_2$
- t_i is symmetric elsewhere*

t_i is symmetric everywhere but $(\{i\} \times \{1,2,3\})^3$.
Every term fails to be symmetric on $(\{0\} \times \{1,2,3\})^3$ or $(\{1\} \times \{1,2,3\})^3$.

Where to go from here?

Local-to-global

- Finish the classification for G-terms
- When is idempotence necessary?
- Does local-to-global fail for Siggers?

Where to go from here?

Local-to-global

- Finish the classification for G-terms
- When is idempotence necessary?
- Does local-to-global fail for Siggers?

Decide(Σ)

- Other efficient algorithms for deciding Σ?
- Example: 'uniform' subpower membership problem algorithm showed $\text{Decide}^{\text{id}}(\text{minority}) \in \text{NP}$ (Kazda, Opršal, Valeriote, Zhuk '19)
- Is there a linear Maltsev condition Σ with $\text{Decide}^{\text{id}}(\Sigma) \notin \text{NP}$?

Thank you!