Quasiorder lattices and Maltsev algebras

Gergő Gyenizse and Miklós Maróti

University of Szeged

Astana-Almaty, 2015. September 8–13.

Part I: Quasiorder lattices of varieties

Definition

The set of **compatible quasiorders** of an algebra **A** is

$$\mathrm{Quo}(\mathbf{A}) = \{\, \alpha \leq \mathbf{A}^2 \mid \alpha \text{ is reflexive and transitive} \,\}.$$

1. A quasiorder $\alpha \subseteq A^2$ is compatible with **A** if
$$(x, y) \in \alpha \implies (p(x), p(y)) \in \alpha$$
for all unary polinomials p of **A**.
2. $\mathrm{Quo}(\mathbf{A})$ forms an (involution) lattice with $\alpha \wedge \beta = \alpha \cap \beta$ and $\alpha \vee \beta = \overline{\alpha \cup \beta}$, where $\overline{\alpha \cup \beta}$ is the transitive closure of $\alpha \cup \beta$.
3. The set $\mathrm{Con}(\mathbf{A})$ of congruences forms a sublattice of $\mathrm{Quo}(\mathbf{A})$.

Goal

Systematic study of the connection between congruence identities, quasiorder identities and Maltsev conditions satisfied by varieties.

Why study compatible quasiorders?

1. More general than congruences.
2. Better behaved than tolerances.
3. Some connection with the constraint satisfaction problem:

For a subdirect power $\mathbf{R} \leq_{\mathrm{sd}} \mathbf{A}^n$ and a closed path

$$p := k_1 \to k_2 \to \cdots \to k_m \to k_1 \quad \text{with} \quad k_i \in \{1, \ldots, n\}$$

define

$$\alpha_p = \bigcup_{i=1}^{\infty} (\eta_{k_1} \circ \eta_{k_2} \circ \cdots \circ \eta_{k_m})^i \quad \text{where} \quad \eta_k = \ker \pi_k.$$

We have $\alpha_p \in \mathrm{Quo}(\mathbf{R})$ and $\alpha_p \vee \eta_{k_1}$ can be computed from the following two-projections:

$$\pi_{k_1 k_2}(R),\ \pi_{k_2 k_3}(R), \ldots, \pi_{k_m k_1}(R).$$

"Prague strategy" iff $\mathrm{range}(p) \subseteq \mathrm{range}(q) \implies \alpha_p \leq \alpha_q$.

Is this study interesting?

Main results:

1. A locally finite variety $\mathcal{V}$ is congruence distributive ($\mathrm{Con}(\mathbf{A})$ is distributive for all $\mathbf{A} \in \mathcal{V}$) if and only if it is quasiorder distributive ($\mathrm{Quo}(\mathbf{A})$ is distributive for all $\mathbf{A} \in \mathcal{V}$).
2. A locally finite variety is congruence modular if and only if it is quasiorder modular.
3. The variety of semilattices is not quasiorder meet semi-distributive (but it is congruence meet semi-distributive).
4. $\mathrm{Quo}(\mathbf{A})$ is not in the lattice quasivariety generated by the congruence lattices $\mathrm{Con}(\mathbf{B})$ for $\mathbf{B} \in \mathrm{HSP}(\mathbf{A})$.
5. For a finite algebra $\mathbf{A}$ in a congruence meet semi-distributive variety $\mathrm{Quo}(\mathbf{A})$ has no sublattice isomorphic to $\mathbf{M}_3$.
6. For a finite algebra $\mathbf{A}$ in a congruence join semi-distributive variety $\mathrm{Quo}(\mathbf{A})$ is also join semi-distributive.

Congruence distributivity

Theorem (B. Jónsson, 1967)

A variety is congruence distributive iff it has Jónsson terms

$$
\begin{aligned}
x \approx p_1(x,x,y) \text{ and } p_n(x,y,y) &\approx y, \\
p_i(x,y,y) \approx p_{i+1}(x,y,y) &\text{ for odd } i, \\
p_i(x,x,y) \approx p_{i+1}(x,x,y) &\text{ for even } i, \text{ and} \\
p_i(x,y,x) \approx x &\text{ for all } i.
\end{aligned}
$$

Theorem (G. Czédli and A. Lenkehegyi, 1983; I. Chajda, 1991)

There is a Maltsev condition charaterizing quasiorder distributivity.

Corollary (G. Czédli and A. Lenkehegyi, 1983)

If a variety $\mathcal{V}$ has a majority term, then it is quasiorder distributive.

Directed Jónsson terms

Definition

The ternary terms $p_1, \ldots, p_n$ are **directed Jónsson terms** if

$$x \approx p_1(x,x,y) \text{ and } p_n(x,y,y) \approx y,$$
$$p_i(x,y,y) \approx p_{i+1}(x,x,y) \text{ for } i = 1,\ldots,n-1, \text{ and}$$
$$p_i(x,y,x) \approx x \text{ for } i = 1,\ldots,n.$$

Theorem (A. Kazda, M. Kozik, R. McKenzie and M. Moore, 2014)

A variety is congruence distributive if and only if it has directed Jónsson terms.

Lemma (A. Kazda, M. Kozik, R. McKenzie and M. Moore, 2014)

If $\alpha \lhd_{\mathrm{WJ}} \beta$ (weak Jónsson absorbs) for $\alpha, \beta \in \mathrm{Quo}(\mathbf{A})$ then $\alpha = \beta$.

Theorem (L. Barto, 2012)

Finitely related algebras in congruence distributive varieties have near unanimity terms.

$$t(y,x,\dots,x) \approx t(x,y,x\dots,x) \approx \cdots \approx t(x,\dots,x,y) \approx x.$$

Theorem

A locally finite variety is congruence distributive if and only if it has directed Jónsson terms.

Proof.

Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x,y)$ be the two-generated free algebra, and put

$$R = \mathrm{Sg}\{(x,x,x),(x,y,y),(y,x,y)\} \le \mathbf{F}^3.$$

The algebra $(F;\mathrm{Pol}(R))$ is finitely related and has Jónsson terms, so R has a near-unanimity polymorphism t. The terms generating the tuples $t((y,x,y),\dots,(y,x,y),(x,y,y),(x,x,x),\dots,(x,x,x))$ are directed Jónsson terms. $\square$

Theorem

If a finite algebra has directed Jónsson terms, then it is quasiorder distributive.

Proof.

1. We show $(\alpha \vee \beta) \wedge \gamma \leq (\alpha \wedge \gamma) \vee (\beta \wedge \gamma)$ for $\alpha, \beta, \gamma \in \mathrm{Quo}(\mathbf{A})$
2. Put $\gamma^* = \gamma \cap \gamma^{-1} \in \mathrm{Con}(\mathbf{A})$
3. Choose $(a, b) \in (\alpha \vee \beta) \wedge \gamma - (\alpha \wedge \gamma) \vee (\beta \wedge \gamma)$ such that the interval $[a/\gamma^*, b/\gamma^*]$ is minimal in the poset $(A/\gamma^*; \gamma/\gamma^*)$
4. We have a chain of $\alpha \cup \beta$ links connecteing a and b
5. Use the directed Jónsson terms to move this chain inside the interval $[a, b] = \{ x \mid a \, \gamma \, x \, \gamma \, b \}$.
6. The links inside a/γ^* are in $(\alpha \wedge \gamma) \cup (\beta \wedge \gamma)$.
7. The first link leaving a/γ^* is also in $(\alpha \wedge \gamma) \cup (\beta \wedge \gamma)$.
8. By minimality the rest is also in $(\alpha \wedge \gamma) \vee (\beta \wedge \gamma)$. □

Theorem

For a locally finite variety $\mathcal{V}$ the following are equivalent:

1. *$\mathcal{V}$ is congruence distributive,*
2. *$\mathcal{V}$ has [directed] Jónsson terms,*
3. *$\mathcal{V}$ is quasiorder distributive.*

Problem

Does the above equivalence hold for all varieties? Does quasiorder distributivity imply directed Jónsson terms syntactically?

Lemma

For a finite algebra with directed Jónsson terms and α, β compatible reflexive relations we have $\overline{\alpha} \cap \overline{\beta} = \overline{\alpha \cap \overline{\beta}}$.

Directed Gumm terms

Definition

The ternary terms $p_1, \dots, p_n, q$ are **directed Gumm terms** if

$$\begin{aligned} x &\approx p_1(x,x,y), \\ p_i(x,y,y) &\approx p_{i+1}(x,x,y) \text{ for } i = 1,\dots,n-1, \\ p_i(x,y,x) &\approx x \text{ for } i = 1,\dots,n, \\ p_n(x,y,y) &\approx q(x,y,y) \text{ and } q(x,x,y) \approx y. \end{aligned}$$

Theorem (A. Kazda, M. Kozik, R. McKenzie and M. Moore, 2014)

A variety is congruence modular if and only if it has directed Gumm terms.

- Has been known for locally finite varieties (M. Kozik)
- Similar trick works to show this (L. Barto: finitely related algebras in congruence modular varietes have edge term)

Congruence modularity

Theorem

If a finite algebra has directed Gumm terms then the lattice of its compatible quasiorders is modular.

- To show $\alpha \leq \gamma \implies (\alpha \vee \beta) \wedge \gamma \leq \alpha \vee (\beta \wedge \gamma)$ we take again a counterexample pair (a, b) with minial distance in γ/γ^*.
- Significantly harder than the distributive case.

Theorem

For a locally finite variety $\mathcal{V}$ the following are equivalent:

1. *$\mathcal{V}$ is congruence modular,*
2. *$\mathcal{V}$ has [directed] Gumm terms,*
3. *$\mathcal{V}$ is quasiorder modular.*

Proposition (I. Chajda, 1991)

In n-permutable varieties compatible quasiorders are congruences.

Transitive closure and congruence modularity

Theorem (G. Czédli, E. Horváth, S. Radeleczki, 2003)

Let $\mathbf{A}$ *be an algebra in a congruence modular variety and* α, β *be tolerances (compatible reflexive and symmetric relation) of* $\mathbf{A}$*. Then* $\overline{\alpha \cap \beta} = \overline{\alpha} \wedge \overline{\beta}$.

Theorem

If $\mathbf{A}$ *is an algebra in a locally finite congruence modular variety and* α, β *are compatible reflexive relation of* $\mathbf{A}$*, then*

$$\overline{\alpha \cap \beta} = \overline{\alpha} \wedge \overline{\beta} \quad \text{and} \quad \overline{\alpha \cup \beta} = \overline{\alpha} \vee \overline{\beta}.$$

So taking the transitive closure is a lattice homomorphism from the set of compatible reflexive relations of $\mathbf{A}$ *onto* $\mathrm{Quo}(\mathbf{A})$.

Lemma

If $\overline{\alpha \cap \beta} = \overline{\alpha} \wedge \overline{\beta}$ *holds for all reflexive relations of an algebra* $\mathbf{A}$*, then* $\mathbf{A}$ *is quasiorder modular.*

Semi-distributivity

Definition

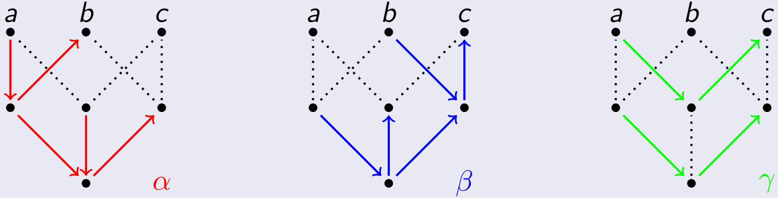
A variety is **congruence meet semi-distributive** if the congruence lattices of its algebras satisfy

$$\alpha \wedge \gamma = \beta \wedge \gamma \implies (\alpha \vee \beta) \wedge \gamma = \alpha \wedge \gamma.$$

The dual condition is **congruence join semi-distributivity**.

Proposition

The variety of semilattices is not quasiorder meet semi-distributive.



Theorem (D. Hobby and R. McKenzie, TCT Theorem 9.10)

For any locally finite variety $\mathcal{V}$ the following are equivalent:

1. $\operatorname{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{2}\} = \emptyset$.
2. *$\mathcal{V}$ satisfies an idempotent linear Maltsev condition that does not hold in the varieties of vectorspaces over finite fields.*
3. $\mathcal{V} \models_{\mathrm{CON}} \gamma \wedge (\alpha \circ \beta) \subseteq \alpha_m \wedge \beta_m$ *for some m where* $\alpha_0 = \alpha$, $\beta_0 = \beta$, $\alpha_{n+1} = \alpha \vee (\gamma \wedge \beta_n)$ *and* $\beta_{n+1} = \beta \vee (\gamma \wedge \alpha_n)$.
4. $\mathbf{M}_3$ *is not a sublattice of* $\mathrm{Con}(\mathbf{A})$ *for any* $\mathbf{A} \in \mathcal{V}$.
5. *$\mathcal{V}$ is congruence meet semi-distributive.*
6. *There are no non-trivial abelian congruences.*

- The previous example shows that $\mathbf{D}_1$ is a sublattice of the quasiorder lattice of the free semilattice with three generators.
- So items (3) and (5) do not hold for quasiorder lattices.

Theorem

For a finite algebra $\mathbf{A}$ *in a congruence meet semi-distributive variety* $\mathrm{Quo}(\mathbf{A})$ *does not have a sublattice isomorphic to* $\mathbf{M}_3$.

Proof.

1. Choose a minimal sublattice of $\mathrm{Quo}(\mathbf{A})$ isomorphic to $\mathbf{M}_3$.
2. The botton quasiorder α cannot have a double edge.
3. The top quasiorder β must have a double edge.
4. The top quasiorder β must be a congruence.
5. The algebra must be (α, β)-minimal.
6. The algebra must be $(0, \beta)$-minimal.
7. Use classification of minimal algebras. □

Theorem

For a finite algebra $\mathbf{A}$ *in a congruence join semi-distributive variety* $\mathrm{Quo}(\mathbf{A})$ *is also join semi-distributive.*

Part II: Algorithms for Maltsev algebras

Constraint satisfaction problem

Definition

For a finite relational structure $\mathbb{B}$ we define

$$\mathrm{CSP}(\mathbb{B}) = \{\, \mathbb{A} \mid \mathbb{A} \to \mathbb{B} \,\}.$$

- CSP() is the class of 3-colorable graphs
- CSP() is the class of bipartite graphs

Dichotomy Conjecture (T. Feder, M. Y. Vardi, 1993)

For every finite structure $\mathbb{B}$ the membership problem for $\mathrm{CSP}(\mathbb{B})$ is in **P** or **NP**-complete.

The dichotomy conjecture is proved for example when $\mathbb{B}$

- is an undirected graph (P. Hell, J. Nešetřil),
- has at most 3 elements (A. Bulatov)

Open for directed graphs (equivalent with the original conjecture).

CSP for Maltsev algebras

Definition

Let $\mathbf{B}$ be an algebra with a Maltsev term p, and $n \in \mathbb{N}$.

- **index** is an element of $\{1, \ldots, n\} \times B^2$,
- an index (i, a, b) is **witnessed** in $Q \subseteq B^n$ if there exist $f, g \in Q$ so that $f_1 = g_1, \ldots, f_{i-1} = g_{i-1}$ and $f_i = a$, $g_i = b$
- a **compact representation** of a subpower $\mathbf{R} \leq \mathbf{B}^n$ is $Q \subseteq R$ that witnesses the same set of indices as $\mathbf{R}$ and $|Q| \leq 2|B|^2 \cdot n$.

Lemma

The compact representation of $\mathbf{R} \leq \mathbf{B}^n$ *generates* $\mathbf{R}$ *as a subalgebra.*

- Idea: take $f \in \mathbf{R}$ and its best approximation $g \in \mathrm{Sg}(Q)$
- let i be the smallest index where $f_i \neq g_i$
- take witnesses $f', g' \in Q$ for the index $(i, f(i), g(i))$
- but then $p(f', g', g)$ is a better approximation of f

CSP for Maltsev algebras

Lemma

The 2-projections of $\mathbf{R} \leq \mathbf{B}^n$ *are polynomial time computable from the compact representation of* $\mathbf{R}$*.*

- Idea: generate as usual, but keep track of representative tuples only

Lemma

For $c_1, \dots, c_k \in B$ *the compact representation of the subpower* $\mathbf{R}' = \{ f \in \mathbf{R} \mid f_1 = c_1, \dots, f_k = c_k \}$ *is poly time computable from that of* $\mathbf{R}$*.*

- Idea: we prove it for $k = 1$ and use induction
- take $f, g \in \mathbf{R}'$ witnesses for (i, a, b) in $\mathbf{R}'$
- then we have witnesses $f', g' \in Q$ for (i, a, b), and
- $h \in \mathrm{Sg}(Q)$ such that $h_1 = c$ and $h_i = a$
- thus $h, p(h, f', g') \in \mathrm{Sg}(Q)$ witness (i, a, b) in $\mathbf{R}'$

CSP for Maltsev algebras

Theorem (A. Bulatov, V. Dalmau, 2006)

Let $\mathbf{B}$ *be a finite algebra with a Maltsev term operation. Then* $\mathrm{CSP}(\mathbf{B})$ *is solvable in polynomial time.*

Theorem

Let $\mathbf{B}$ *be a finite Maltsev algebra. Then the compact representation of the product, projection and intersection of subpowers is computable in polynomial time from the compact representations of the arguments.*

Idea: intersection $\mathbb{R} \cap \mathbb{S}$ can be computed by taking the product $\mathbb{R} \times \mathbb{S}$ then applying equality constraints then a projection.

Question: can the compat representation be computed for the join (generated subalgebra of the union) of two relations?

Subpower membership problem

Problem

The subpower membership problem for a fixed finite algebra $\mathbf{A}$ *is the problem of deciding for a set* $X \subseteq A^n$ *and* $f \in A^n$ *decide* $f \in \mathrm{Sg}(X)$.

1. Naive algorithm: EXPTIME
2. There exists $\mathbf{A}$ for which $\mathrm{SMP}(\mathbf{A})$ is EXPTIME-complete (Kozik 2008)
3. $\mathrm{SMP}(\mathbf{A})$ is in P for groups and rings (Sims 1971; Furst, Hopcroft, Luks 1980)
4. There exists a 3-element semigroup $\mathbf{A}$ for which $\mathrm{SMP}(\mathbf{A})$ is NP-complete (Bulatov 2013)
5. Complete characterization of $\mathrm{SMP}(\mathbf{A})$ for commutative and 0-simple semigroups (Bulatov, Mayer, Steindl 2015)
6. Open for Maltsev algebras (Willard 2007)

Subpower membership for groups

- Fix a finite group $\mathbf{G}$ and suppose, that $\mathbf{R} \leq \mathbf{G}^n$.
- We know, that $(1, \dots, 1) \in R$, so we can search for $(i, 1, a)$ forks between $(1, \dots, 1)$ and $(1, \dots, 1, a, -, \dots, -)$.
- Let Q_i be a representation of all $(i, 1, -)$ forks, and put $Q = \bigcup_{i=1}^n Q_i$.
- Q is small and $R = Q_1 Q_2 \cdots Q_n$ (unique representation)
- Problem: find this compact representation for $\mathbf{R}$ from a generating set $X \subseteq G^n$
- We can incrementally do this, and stop when $Q_i Q_j \subseteq Q_1 \cdots Q_n$, because then we are guaranteed that $Q_1 \cdots Q_n$ is then a subgroup.
- Open: how to check if $Q_1 \cdots Q_n$ is closed under another operation than the product?

Computation with congruences

Definition

Let α, β be congruences of an algebra $\mathbf{R}$. A **transversal of** α **modulo** β is a set $T \subseteq \alpha$ of cardinality at most $|(\alpha \vee \beta)/\beta|$ such that $\alpha \vee \beta = \overline{T \cup \beta}$.

Lemma

Let $\mathbf{A}$ *be a Maltsev algebra,* $\mathbf{R} \leq \mathbf{A}^n$ *be a subpower and* $\eta_1, \dots, \eta_n$ *be the projection kernels in* $\mathrm{Con}(\mathbf{A})$*. If* T_i *is a traversal of* $\eta_1 \wedge \ldots \wedge \eta_{i-1}$ *modulo* η_i*, then* $\bigcup_{i=1}^{n} T_i$ *generates* $\mathbf{R}$*.*

Lemma

Let α, β *be congruences of an algebra* $\mathbf{A}$ *with a modular congruence lattice. If* T *is a transversal of* α *modulo* β*, then* $\alpha = (\alpha \wedge \beta) \vee \mathrm{Cg}_{\mathbf{A}}(T)$*.*

Computation with congruences

Lemma

Let α, β, γ be congruences of an algebra $\mathbf{R}$ with a modular congruence lattice. Then a transversal of α modulo $\beta \wedge \gamma$ can be computed from transversals of α modulo β, $\alpha \wedge \beta$ modulo γ and $A/(\beta \wedge \gamma)$.

Lemma

Let α, β, γ be congruences of an algebra $\mathbf{R}$ with a modular congruence lattice. Then a transversal of $\alpha \wedge \beta$ modulo γ can be computed from a transversal of α modulo $\beta \wedge \gamma$.

Corollary

If we have a compact representation of $\mathbf{R} \leq \mathbf{A}^n$ for an algebra in a congruence modular variety, then we can permute the coordinates of $\mathbf{R}$ and compute the compact representation of the new relation.

The unknown case

- We can assume, that we have the traversals (compact representations) for all indices except for the last one.
- We can assume, that η_n is meet irreducible (otherwise break it up into more coordinates) and that $\eta_1 \wedge \ldots \wedge \eta_{n-1} \leq \eta_n^*$.
- We can assume that $\eta_n^* = \eta_1$ by rearranging and combining coordinates.
- We can assume, that $\eta_2, \ldots, \eta_{n-1}$ are also meet irreducible, and $\eta_1 \wedge \ldots \wedge \eta_{i-1} \wedge \eta_{i+1} \wedge \ldots \wedge \eta_{n-1} = \eta_i^*$.
- We can assume, that the transversals (one fork) of $\eta_1 \wedge \ldots \wedge \eta_{i-1} \wedge \eta_{i+1} \wedge \ldots \wedge \eta_{n-1}$ modulo η_i are also a transversals modulo η_n, so their n-th coordinates are different.
- Can we decide whether $\eta_1 \wedge \ldots \wedge \eta_n = 0$ or find a fork?

Thank You!