Similarity, ~~critical relations~~, and Zhuk's bridges

Ross Willard

University of Waterloo

AAA 98
Dresden, 21.06.2019

Two happy guys

Andrei Bulatov Dmitriy Zhuk

The CSP Dichotomy Conjecture is solved!

2017: Bulatov and Zhuk independently announce positive solutions to the *Constraint Satisfaction Problem Algebraic Dichotomy Conjecture.*

Their proofs (101 and 47 pages) are on the arXiv.

They analyze invariant relations of finite idempotent Taylor algebras.

Crucial piece: relations that encode hidden linear equations.

Another happy guy

Ralph Freese

R. Freese, "Subdirectly irreducible algebras in modular varieties" (1982)

Topic: subdirectly irreducible algebras (SIs) with <u>abelian</u> monolith in congruence modular (CM) varieties, especially:

- linear coordinatization of monolith-classes;
- a "similarity relation" (compatibility of coordinatizations).

Goals of this lecture:

1. Recall some of Freese's results.
2. ~~Recall a related result of Kearnes & Szendrei.~~
3. Announce that these results extend to finite SIs in Taylor varieties.
4. Connect everything to one aspect of Zhuk's CSP proof.

Basic definitions

Let $\mathbf{A}$ be any algebra. Let $\alpha, \beta \in \operatorname{Con} \mathbf{A}$.

Definition.
α centralizes β $\iff$ $\forall$ term $t(\mathbf{x}, \mathbf{y})$, $\forall (a_i, b_i) \in \alpha$, $\forall (c_j, d_j) \in \beta$,

$$t(\mathbf{a}, \mathbf{c}) = t(\mathbf{a}, \mathbf{d}) \iff t(\mathbf{b}, \mathbf{c}) = t(\mathbf{b}, \mathbf{d}).$$

Also write $[\alpha, \beta] = 0$ to mean "α centralizes β."

"α is abelian" $\iff$ $[\alpha, \alpha] = 0$.

"$\mathbf{A}$ is abelian" $\iff$ $[1, 1] = 0$.

Definition.
Given $\beta \in \operatorname{Con} \mathbf{A}$, the centralizer (or annihilator) of β, denoted $(0 : \beta)$, is the largest α such that $[\alpha, \beta] = 0$.

CHAPTER 1

Finite SIs in Congruence Modular varieties

Coordinatization

Theorem 1 (Freese, 1982)

Suppose $\mathbf{A}$ is a finite SI algebra with abelian monolith μ in a CM variety. There exists a term $d(x, y, z)$ and a prime p such that:

1. $\forall$ μ-class C, $\exists$ $k = k_C$ such that $(C, d|_{C^3}) \cong ((\mathbb{Z}_p)^k, x{-}y{+}z)$. (This is "coordinatization of C." Notation: $C \leftrightsquigarrow (\mathbb{Z}_p)^k$)
2. Every n-ary polynomial operation of $\mathbf{A}$, when restricted to an n-tuple of μ-classes, is *affine* (linear-plus-a-constant) with respect to these coordinatizations.

Special case: if $\mathbf{A}$ is finite simple and abelian, then $\mathbf{A}$ is term-equivalent to a reduct of a vector space over $\mathbb{Z}_p$ with additional affine operations.

Compact coordinatization: special case

Theorem 2_s (Freese, 1982)

Suppose $\mathbf{A}$ is a finite SI algebra with abelian monolith μ in a CM variety.

Assume $(0 : \mu) = 1$. (Consider μ as a subalgebra $\boldsymbol{\mu} \leq \mathbf{A}^2$.)

There exists a simple abelian algebra $\mathbf{D} \leftrightsquigarrow (\mathbb{Z}_p)^k$, a subuniverse $\{o\} \leq \mathbf{D}$, and a surjective homomorphism $h : \boldsymbol{\mu} \twoheadrightarrow \mathbf{D}$ such that:

1. Every μ-class C is $\leftrightsquigarrow D$ via $x \mapsto h(x, a)$ (any fixed $a \in C$).
2. $h^{-1}(o) = \{(a, a) : a \in A\} = 0_A$.

Moreover, $(\mathbf{D}, o)$ is unique up to isomorphism.

Intuition:

$\mathbf{D}$ uniformly coordinatizes the μ-classes of $\mathbf{A}$ via h;

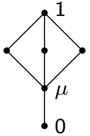
$\{o\}$ distinguishes 0_A inside μ.

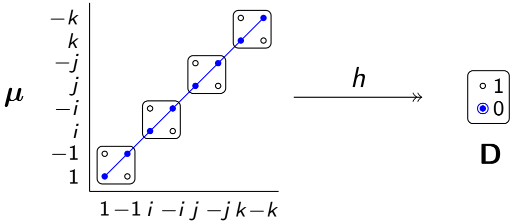
$$\begin{tikzcd} \boldsymbol{\mu} \arrow[r, two heads, "h"] & \mathbf{D} \\ 0_A \arrow[u, hook] \arrow[r, dashed, two heads] & \{o\} \arrow[u, hook] \end{tikzcd}$$

Example

Let $\mathbf{A}$ = the quaternion group $\mathbf{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

- $\mathbf{Q}_8$ is SI, monolith μ is abelian.
- $(0 : \mu) = 1$.
- μ has classes $\{\pm 1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}$.
- Theorem 2_s is witnessed by the simple group $\mathbf{D} = \mathbb{Z}_2$ and $\{o\} = \{0\}$.
- $h : \boldsymbol{\mu} \twoheadrightarrow \mathbf{D}$ sends all $(x, x) \mapsto 0$ and all $(x, -x) \mapsto 1$.





Compact coordinatization – general case

Theorem 2 (Freese, 1982)

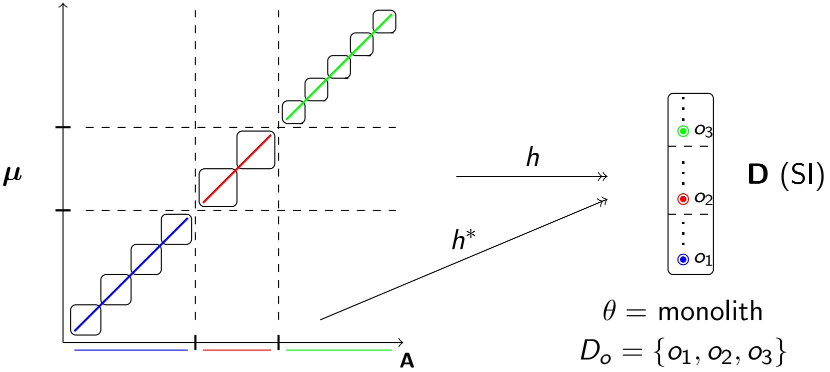
Suppose $\mathbf{A}$ is a finite SI algebra with abelian monolith μ in a CM variety.

Then (…something similar to Theorem 2_s but more complicated…).

Theorem 2_s	Theorem 2
Assume $(0:\mu)=1$.	Let $\boxed{(0:\mu)=\alpha.}$ (Note $\alpha \geq \mu$)
$\exists$ simple abelian $\mathbf{D}$	$\exists$ SI $\mathbf{D}$ with abelian monolith θ
$\exists\ \{o\} \leq \mathbf{D}$	$\exists\ D_o \leq \mathbf{D}$, D_o is a transversal for θ
$\exists\ h : \boldsymbol{\mu} \twoheadrightarrow \mathbf{D}$	$\exists\ h : \boldsymbol{\mu} \twoheadrightarrow \mathbf{D}$ and $h^* : \mathbf{A}/\alpha \cong \mathbf{D}/\theta$ compatible, i.e., $h(a,b)/\theta = h^*(a/\alpha) = h^*(b/\alpha)$
$C \leftrightsquigarrow D\ \forall C \in A/\mu$	$C \in A/\mu$, $C \subseteq S \in A/\alpha$, $h^*(S) = T \implies C \leftrightsquigarrow T$
$h^{-1}(o) = 0_A$	$h^{-1}(D_o) = 0_A$
$(\mathbf{D}, o)$ unique$/\cong$	$(\mathbf{D}, D_o)$ unique$/\cong$

Picture

A finite SI in CM variety, abelian monolith μ, $(0 : \mu) = \alpha$



$h^* : \mathbf{A}/\alpha \;\cong\; \mathbf{D}/\theta$

Comparing coordinatizations: Similarity

In the same paper, Freese defined a similarity relation $\sim$ on SIs.

It's complicated.

Equivalent characterization (Freese)

Let $\mathbf{A}_1$ and $\mathbf{A}_2$ be finite SIs with abelian monoliths in a CM variety.

$\mathbf{A}_1$ is similar to $\mathbf{A}_2$, written $\mathbf{A}_1 \sim \mathbf{A}_2$, $\iff$

$\exists$ $(\mathbf{D}, D_o)$ which witnesses Theorem 2 for both $\mathbf{A}_1$ and $\mathbf{A}_2$.

Examples:

1. $\mathbf{Q}_8 \sim \mathbb{Z}_4$. $(\mathbb{Z}_2, \{0\})$ witnesses Theorem 2 for both.
2. $\mathbf{S}_3 \sim \mathbb{Z}_9$? No. $(0 : \mu_{\mathbf{S}_3}) = \mu_{\mathbf{S}_3}$ while $(0 : \mu_{\mathbb{Z}_9}) = 1$.

In general, $\mathbf{A}_1 \sim \mathbf{A}_2 \implies \mathbf{A}_1/\alpha_1 \cong \mathbf{A}_2/\alpha_2$ where $\alpha_i = (0 : \mu_i)$.

Freese gave other characterizations of similarity.

Here is a new one.

Theorem 3 (W)

Let $\mathbf{A}, \mathbf{B}$ be finite SI algebras with abelian monoliths $\mu_{\mathbf{A}}, \mu_{\mathbf{B}}$ in a CM variety. $\mathbf{A} \sim \mathbf{B} \iff \exists\, R \leq \mathbf{A} \times \mathbf{A} \times \mathbf{B} \times \mathbf{B}$ satisfying:

1. $\mathrm{proj}_{1,2}(R) = \mu_{\mathbf{A}}$ and $\mathrm{proj}_{3,4}(R) = \mu_{\mathbf{B}}$.
2. $(a_1, a_2, b_1, b_2) \in R$ implies $(a_1 = a_2 \iff b_1 = b_2)$.
3. $(a_1, a_2, b_1, b_2) \in R$ implies $(a_i, a_i, b_i, b_i) \in R$ for $i = 1, 2$.

Proof idea for $(\Rightarrow)$:

- Let $(\mathbf{D}, D_o)$ and $h_{\mathbf{A}} : \boldsymbol{\mu}_{\mathbf{A}} \twoheadrightarrow \mathbf{D}$, $h_{\mathbf{B}} : \boldsymbol{\mu}_{\mathbf{B}} \twoheadrightarrow \mathbf{D}$ witness $\mathbf{A} \sim \mathbf{B}$.
- Define $R = \{(a_1, a_2, b_1, b_2) \,:\, h_{\mathbf{A}}(a_1, a_2) = h_{\mathbf{B}}(b_1, b_2)\}$.

Critical relations

Now consider relations that encode linear equations.

Example: $\rho \leq_{sd} (\mathbb{Z}_p)^n$ given by $\rho = \{(x_1, \ldots, x_n) : x_1 + \cdots + x_n = 0\}$.

What formal properties do such relations have?

Definition

Suppose $\mathbf{A}_1, \ldots, \mathbf{A}_n$ are finite and $\rho \leq_{sd} \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$.

1. ρ is **critical** if
   1. there is no partition $\{1, \ldots, n\} = X \cup Y$ so that ρ is the product of its projections onto X and Y;
   2. ρ is meet-irreducible in the lattice of subuniverses of $\mathbf{A}_1 \times \cdots \times \mathbf{A}_n$.
2. ρ is **fork-free** if there do not exist $\mathbf{a}, \mathbf{b} \in \rho$ which differ at exactly one coordinate.

Critical relations yield similarity

Theorem 4 (Kearnes & Szendrei, 2012)

Suppose $\rho \leq_{sd} \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ is critical and fork-free, where $\mathbf{A}_1, \ldots, \mathbf{A}_n$ are finite algebras in a CM variety. If $n \geq 3$, then:

1. Each $\mathbf{A}_i$ is SI with abelian monolith.
2. $\mathbf{A}_i \sim \mathbf{A}_j$ for all i, j.

CHAPTER 2

Finite SIs in Taylor[1] varieties

[1] Varieties satisfying the weakest nontrivial idempotent Maltsev condition

Theorems 1 and 2 extend[2] to Taylor varieties!

Theorem 1^+ (Folklore?)

Suppose $\mathbf{A}$ is a finite SI with abelian monolith μ in a Taylor variety.

1. $\exists$ term $d(x, y, z)$ and prime p exactly as before.
2. Polynomials restrict to μ-classes exactly as before.

Theorem 2^+ (new?)

Suppose $\mathbf{A}$ is a finite SI with abelian monolith μ in a Taylor variety.

Let $\alpha = (0 : \mu)$.

$\exists$ SI $\mathbf{D}$ with abelian monolith θ, $D_o \leq \mathbf{D}$, $h : \boldsymbol{\mu} \twoheadrightarrow \mathbf{D}$, $h^* : \mathbf{A}/\alpha \cong \mathbf{D}/\theta$ exactly as before, except

- The coordinatization maps $x \mapsto h(x, a)$ are <u>injections</u> $C \hookrightarrow T$ ($C \in A/\mu$, $T \in D/\theta$) instead of bijections $C \leftrightsquigarrow T$.

[2] One minor change to Theorem 2

Extending $\sim$ to Taylor varieties

Freese's characterization of $\sim$ via Theorem 2 suggests the following:

Definition.

Let $\mathbf{A}_1$ and $\mathbf{A}_2$ be finite SIs with abelian monoliths in a Taylor variety.

Say $\mathbf{A}_1$ is <u>similar</u> to $\mathbf{A}_2$, and write $\mathbf{A}_1 \sim \mathbf{A}_2$, if $\exists$ $(\mathbf{D}, D_o)$ which witnesses Theorem 2^+ for both $\mathbf{A}_1$ and $\mathbf{A}_2$.

This extends the usual $\sim$ from CM varieties.

Theorems 3 and $\cancel{4}$ extend to Taylor varieties!

Theorem 3^+ (W)

Let $\mathbf{A}, \mathbf{B}$ be finite SI algebras with abelian monoliths $\mu_{\mathbf{A}}, \mu_{\mathbf{B}}$ in a Taylor variety. $\mathbf{A} \sim \mathbf{B} \iff \exists$ a 4-ary witness $R \leq \mathbf{A} \times \mathbf{A} \times \mathbf{B} \times \mathbf{B}$ as before:

1. $\mathrm{proj}_{1,2}(R) = \mu_{\mathbf{A}}$ and $\mathrm{proj}_{3,4}(R) = \mu_{\mathbf{B}}$.
2. $(a_1, a_2, b_1, b_2) \in R$ implies $(a_1 = a_2 \iff b_1 = b_2)$.
3. $(a_1, a_2, b_1, b_2) \in R$ implies $(a_i, a_i, b_i, b_i) \in R$ for $i = 1, 2$.

~~**Theorem 4^+ (W)**~~

~~Suppose $\rho \leq_{sd} \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ is critical and fork-free, where $\mathbf{A}_1, \ldots, \mathbf{A}_n$ are finite algebras in a Taylor variety. If $n \geq 3$, then (exactly as before...)~~

Proofs: use Tame Congruence Theory.

CHAPTER 3

Zhuk's bridges

D. Zhuk, "A proof of CSP Dichotomy Conjecture"

`arXiv:1704.01914`

Let $\mathbf{A}$ be a finite SI with monolith μ in a Taylor variety. Let $0 = 0_A$.

Zhuk defines:	TCT equivalent
"0 is irreducible" $\iff$ 0 is meet-irreducible in $\mathrm{Sub}(\mathbf{A}^2)$	$\mathrm{typ}(0, \mu) \in \{2, 3\}$
Assume 0 is irreducible:	
$0^* :=$ the cover of 0 in $\mathrm{Sub}(\mathbf{A}^2)$	basic tolerance for $(0, \mu)$
$\mathrm{Opt}(0) :=$ (a certain congruence of $\mathbf{A}$)	$(0 : \mu)$

Suppose $\mathbf{A}, \mathbf{B}$ are finite SIs with monoliths $\mu_{\mathbf{A}}, \mu_{\mathbf{B}}$ in a Taylor variety.

Assume 0_A and 0_B are irreducible.

Definition (Zhuk).
A bridge from 0_A to 0_B is a relation $R \leq \mathbf{A} \times \mathbf{A} \times \mathbf{B} \times \mathbf{B}$ satisfying

1. $\mathrm{proj}_{1,2}(R) \supseteq 0_A^*$ and $\mathrm{proj}_{3,4}(R) \supseteq 0_B^*$.
2. $(a_1, a_2, b_1, b_2) \in R$ implies $(a_1 = a_2$ iff $b_1 = b_2)$.

Let's define a bridge to be restricted if the two $\supseteq$'s in 1 are $=$'s.

In effect, Zhuk uses only restricted bridges.

A restricted bridge from 0_A to 0_B is any $R \leq \mathbf{A} \times \mathbf{A} \times \mathbf{B} \times \mathbf{B}$ satisfying

1. $\mathrm{proj}_{1,2}(R) = 0_A^*$ and $\mathrm{proj}_{3,4}(R) = 0_B^*$.
2. $(a_1, a_2, b_1, b_2) \in R$ implies $(a_1 = a_2$ iff $b_1 = b_2)$.

Now assume that $\mu_{\mathbf{A}}, \mu_{\mathbf{B}}$ are abelian.

Then $0_A^* = \mu_{\mathbf{A}}$ and $0_B^* = \mu_{\mathbf{B}}$. (By Theorem 1^+)

Thus (in this case) a restricted bridge from 0_A to 0_B is a relation $R \leq \mathbf{A} \times \mathbf{A} \times \mathbf{B} \times \mathbf{B}$ satisfying

1. $\mathrm{proj}_{1,2}(R) = \mu_{\mathbf{A}}$ and $\mathrm{proj}_{3,4}(R) = \mu_{\mathbf{B}}$.
2. $(a_1, a_2, b_1, b_2) \in R$ implies $(a_1 = a_2$ iff $b_1 = b_2)$.

OMG!!! This is 2/3rds of my Theorem 3^+ characterization of $\mathbf{A} \sim \mathbf{B}$.

(Missing: the property $(a_1, a_2, b_1, b_2) \in R \implies (a_i, a_i, b_i, b_i) \in R$.)

OMG!!! All (restricted) bridges used by Zhuk satisfy this extra property.

Conclusion: Zhuk's bridges witness similarity.

Zhuk's bridges and critical relations

Theorem 8.15 (Zhuk), very special case

Suppose $\rho \leq_{sd} \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ is critical and fork-free, where $\mathbf{A}_1, \ldots, \mathbf{A}_n$ are finite algebras in a Taylor variety. If $n \geq 3$, then for all $i \neq j$ there exists a [restricted] bridge R_{ij} from 0_{A_i} to 0_{A_j} [with the additional property].

OMG!!! It's Theorem 4^+, and $\mathbf{A}_1 \sim \cdots \sim \mathbf{A}_n$.

Moreover, Zhuk's analysis implies that for fixed i, $\mathrm{Opt}(0_{A_i})$ contains all pairs (a, a') where a, a' are "linked in ρ," i.e., connected by a path with edges in $\bigcup_{j \neq k} \mathrm{proj}_{j,k}(\rho)$.

OMG!!! Linkedness pushes $(0 : \mu_i)$ towards 1.

Most of Zhuk's CSP dichotomy proof works for arbitrary (idempotent) finite algebras in a Taylor variety. However, a few places require the following:

Assumption: $\mathbf{A} = (A, w)$ where w is an m-ary "special WNU".

For example:

Theorem 8.10 (Zhuk), special case

Assume $\mathbf{A} = (A, w)$ satisfies this assumption, $\mathbf{A}$ is SI with monolith μ, 0_A is irreducible, and $\mathrm{Opt}(0_A) = 1$. Then $\exists$ a prime p and a surjective homomorphism $h : \mathbf{0}_{\boldsymbol{A}}^* \twoheadrightarrow (\mathbb{Z}_p, x_1 + \cdots + x_m)$ with $h^{-1}(0) = 0_A$.

Recall: $\mathrm{Opt}(0_A) = (0_A : \mu)$. So $(0_A : \mu) = 1$. So μ is abelian. So $\mathbf{0}_{\boldsymbol{A}}^* = \boldsymbol{\mu}$.

OMG!!! Zhuk's Theorem 8.10 is an instance of Theorem 2_s^+.

Conclusion

The parts of Zhuk's analysis using bridges and Opt can be viewed as instances of similarity and centralizers in Taylor varieties.

The parts that require the special WNU assumption (previous slide) can be relaxed to any idempotent algebras in Taylor varieties.

Thus Zhuk's algorithm can be adapted to apply directly to any finite idempotent algebra with a Taylor term.

Thank you!