The Constraint Satisfaction Dichotomy Theorem for Beginners

Tutorial – Part 2

Ross Willard

University of Waterloo

BLAST 2019
CU Boulder, May 22, 2019

Recall:

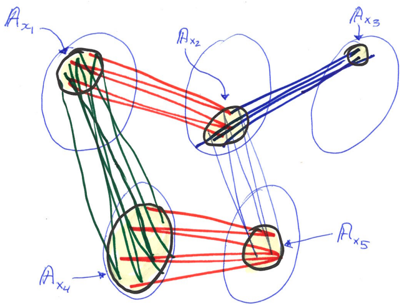
An algebra $\mathbb{A} = (A, \mathcal{F})$ is:

- idempotent if every $f \in \mathcal{F}$ satisfies $(\forall x)\ f(x, x, \ldots, x) = x$.
- Taylor if it is idempotent and has a term operation $t(x_1, \ldots, x_n)$ satisfying identities of the form $(\forall x, y \ldots)\ t(\mathrm{vars}) = t(\mathrm{vars}')$ forcing t to not be a projection.

A (multi-sorted) CSP instance compatible with $\mathbb{A}$ consists of

- a family $(\mathbb{A}_{x_i} : 1 \leq i \leq n)$ of subalgebras of $\mathbb{A}$ (indexed by variables), and
- a set $\{C_t\ :\ 1 \leq t \leq m\}$ of "constraints" of the form $R_t(x_{i_1}, \ldots, x_{i_k})$ where

$$R_t \leq_{sd} \mathbb{A}_{x_{i_1}} \times \cdots \times \mathbb{A}_{x_{i_k}}.$$



Assuming Θ is a CSP instance compatible with a Taylor algebra $\mathbb{A}$ and satisfying some level of local consistency,

How can Θ nonetheless be inconsistent?

One obvious way: if it encodes linear equations.

Plan for today: to explain in detail how compatible subdirect relations of Taylor algebras encode linear equations.

- In particular, the role of:
    - abelian congruences
    - critical rectangular relations
    - strands
    - similarity

I will explain by examples, using "Maltsev reducts of groups."

Definition

Given a group $\mathbb{G}$, its <u>Maltsev reduct</u> is the algebra $\mathbb{G}^{aff} = (G, xy^{-1}z)$.

Note:

1. $\mathbb{G}^{aff}$ is Taylor.
2. $\mathbb{G}$ and $\mathbb{G}^{aff}$ have the same congruences.
3. The relations compatible with $\mathbb{G}^{aff}$ are any cosets (left or right) of subgroups $H \leq \mathbb{G} \times \cdots \times \mathbb{G}$.

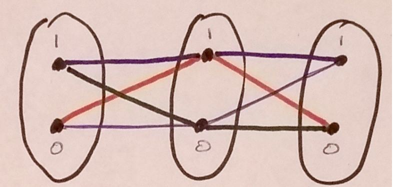
Example 1: $\mathbb{Z}_p$

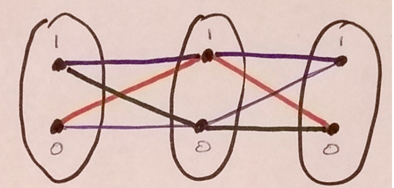
We've already seen $\mathbb{Z}_p^{aff} = (\mathbb{Z}_p,\ x{-}y{+}z)$.

$$\mathrm{Norm}\,\mathbb{Z}_p = \begin{array}{l} \bullet\ \mathbb{Z}_p \\ | \\ \bullet\ \{0\} \end{array} \qquad \text{so} \qquad \mathrm{Con}\,\mathbb{Z}_p^{aff} = \begin{array}{l} \bullet\ 1 \text{ (abelian)} \\ | \\ \bullet\ 0 \end{array}$$

A relation compatible with $\mathbb{Z}_2^{aff}$ is

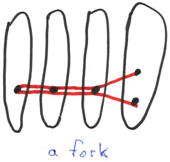
$$L_{111} \;=\; \{(x,y,z) \in (\mathbb{Z}_2)^3 \;:\; x+y+z=1\}.$$

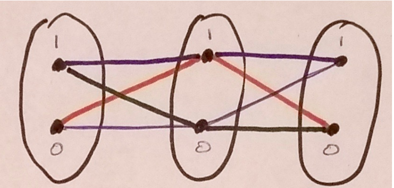




Observe that the relation L_{111} has the following properties:

1. L_{111} is subdirect.
2. L_{111} is "functional at every variable."
    - This is equivalent to L_{111} being fork-free, where a fork is a pair of elements in the relation which disagree at exactly one coordinate.





Other properties of L_{111}:

3. L_{111} is indecomposable: there is no partition of its coordinates such that L_{111} is the product of its projections onto the two subsets.

4. L_{111} is maximal in the lattice of subuniverses of $\mathbb{Z}_2^{aff} \times \mathbb{Z}_2^{aff} \times \mathbb{Z}_2^{aff}$.

The unique strand of this relation is $\{0,1\} \times \{0,1\} \times \{0,1\}$.

Example 2: $\mathbb{S}_3$

Consider the symmetric group $\mathbb{S}_3$ of order 6:

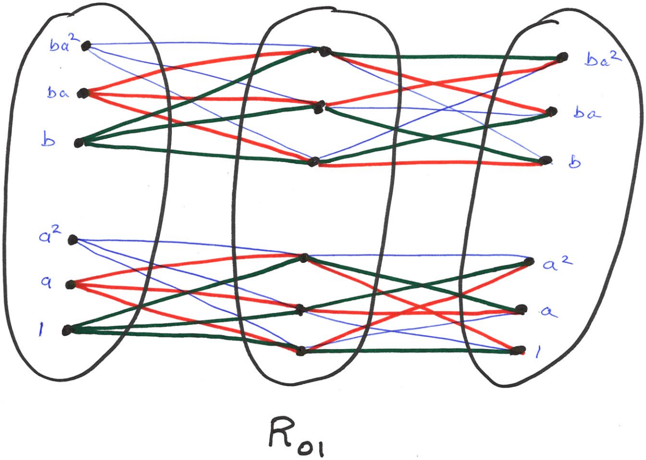
$$\begin{aligned} \mathbb{S}_3 &= \langle a, b \mid a^3 = b^2 = 1,\ ab = ba^{-1} \rangle \\ &= \{1, a, a^2\} \cup \{b, ba, ba^2\}. \end{aligned}$$

$$\operatorname{Norm}\mathbb{S}_3 = \begin{array}{l} \bullet\ S_3 \\ | \\ \bullet\ N \\ | \\ \bullet\ \{1\} \end{array} \qquad \text{so} \qquad \operatorname{Con}\mathbb{S}_3^{aff} = \begin{array}{l} \bullet\ 1 \\ | \\ \bullet\ \equiv_N \text{ (abelian)} \\ | \\ \bullet\ 0 \end{array}$$

Let $R^* = \{(x, y, z) \in (S_3)^3 \,:\, x \equiv_N y \equiv_N z\}$.

For each $c, d \in \mathbb{Z}_3$ let

$$\begin{aligned} R_{cd} &= \{(a^i, a^j, a^k) \,:\, i + j + k = c \pmod 3\} \\ &\cup \{(ba^i, ba^j, ba^k) \,:\, i + j + k = d \pmod 3\}. \end{aligned}$$



Observe that:

- R_{01} is subdirect, fork-free and indecomposable.
- R_{01} supports two distinct (and disjoint) strands:

$$N \times N \times N \qquad \text{and} \qquad N^c \times N^c \times N^c.$$

$$
\begin{aligned}
R_{01} &= \{(a^i, a^j, a^k) \,:\, i+j+k = 0 \pmod 3\} \\
&\cup \{(ba^i, ba^j, ba^k) \,:\, i+j+k = 1 \pmod 3\}.
\end{aligned}
$$

One more property:

- R_{01} is meet-irreducible in the subuniverse lattice of $\mathbb{S}_3^{aff} \times \mathbb{S}_3^{aff} \times \mathbb{S}_3^{aff}$.

Proof sketch.

Recall $R^* = \{(x, y, z) \in (S_3)^3 \,:\, x \equiv_N y \equiv_N z\}$.

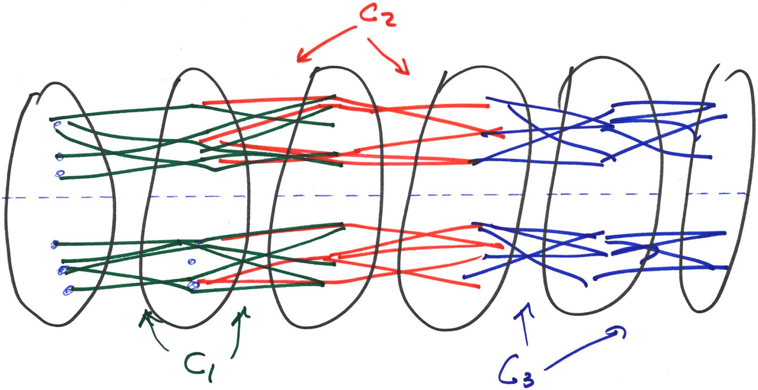
Claim: R^* is the unique minimal subuniverse properly containing R_{01}.

First, it's easy to see that R_{01} is maximal in R^*.

Suppose B is a subuniverse of $(\mathbb{S}_3^{aff})^3$ containing R_{01} and some $\mathbf{x} \notin R^*$. WLOG, $\mathbf{x} = (b, a, a^2)$. Also note that $(a, a, a) \in R_{01}$.

Then $(b, a, a^2)(a, a, a)^{-1}(b, a, a^2) = (a, a, 1) \in B \cap (R^* \setminus R_{01})$. $\square$

Using the R_{cd}'s, we can encode <u>two</u> systems of linear equations over $\mathbb{Z}_3$ on **parallel strands** through cosets of N.



From a CSP perspective, such parallel systems are easily solved.

Example 3: $\mathbb{SL}(2,5)$

Let $\mathbb{G} = \mathbb{SL}(2,5)$ (the group of $M \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}_5)$ with $\det(M) = 1$).

$|G| = 120, \quad Z(\mathbb{G}) = \{1,-1\}, \quad$ and $\mathbb{G}/Z(\mathbb{G}) \cong \mathbb{A}_5$. Let $N = \{1,-1\}$.

$$\mathrm{Norm}\,\mathbb{G} = \begin{array}{l} \bullet\, SL(2,5) \\ \big| \\ \bullet\, N \\ \big| \\ \bullet\, \{1\} \end{array} \qquad \text{so} \qquad \mathrm{Con}\,\mathbb{G}^{aff} = \begin{array}{l} \bullet\, 1 \\ \big| \\ \bullet\, \mu \text{ (abelian)} \\ \big| \\ \bullet\, 0 \end{array}$$

Let $G(\mu) = \{(x,y) \in G^2 : x\,\mu\,y\} \leq \mathbb{G}^2$. Define the map $h : G(\mu) \to \mathbb{Z}_2$ by

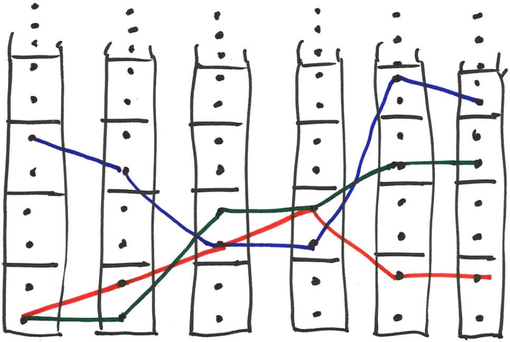
$$h((x,y)) = \begin{cases} 0 & \text{if } x = y \\ 1 & \text{otherwise (i.e., } x = -y). \end{cases}$$

It is a homomorphism $\mathbb{G}(\mu) \to \mathbb{Z}_2$ (because N is central).

Thus we can define

$$
\begin{aligned}
R^* &= G(\mu)^3 \\
R_0 &= \{(\mathbf{x},\mathbf{y},\mathbf{z}) \in G(\mu)^3 : h(\mathbf{x})+h(\mathbf{y})+h(\mathbf{z}) = 0\} \\
R_1 &= \{(\mathbf{x},\mathbf{y},\mathbf{z}) \in G(\mu)^3 : h(\mathbf{x})+h(\mathbf{y})+h(\mathbf{z}) = 1\}
\end{aligned}
$$

all viewed as 6-ary relations compatible with $\mathbb{G}^{aff}$.



R_0

Properties of R_0 and R_1:

1. Each is subdirect, fork-free and indecomposable.
2. Each is meet-irreducible in the subuniverse lattice of $(\mathbb{G}^{aff})^6$. $R^* = G(\mu)^3$ is their common upper cover (exercise).
3. Each supports 3,600 distinct strands, each of the form

$$A^2 \times B^2 \times C^2$$

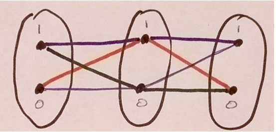
   where A, B, C are μ-classes (cosets of N).
4. Restricted to any strand, R_0 or R_1 defines a linear equation.
5. The strands "cross" each other; CSPs do not parallelize this time.

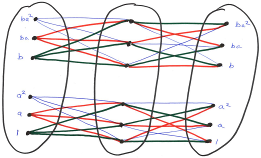
This is the interesting situation; doesn't reduce to simpler scenarios.

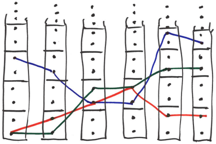
It turns out that strands being "fully linked" (like this example) is connected to the commutator condition $[1, \mu] = 0$.

Summary of the 3 examples

1. $L_{111} \leq \mathbb{Z}_2^{aff} \times \mathbb{Z}_2^{aff} \times \mathbb{Z}_2^{aff}$
2. $R_{01} \leq \mathbb{S}_3^{aff} \times \mathbb{S}_3^{aff} \times \mathbb{S}_3^{aff}$
3. $R_0 \leq \mathbb{G}^{aff} \times \mathbb{G}^{aff} \times \mathbb{G}^{aff} \times \mathbb{G}^{aff} \times \mathbb{G}^{aff} \times \mathbb{G}^{aff}$ where $\mathbb{G} = \mathbb{SL}(2,5)$.







Common properties:

1. Potatoes $\mathbb{A}$ are subdirectly irreducible (SI).
2. Relations R are compatible, subdirect.
3. Relations are fork-free.
4. Relations are indecomposable and meet-irreducible (= critical).
5. The minimal upper cover R^* of the relation R is the coordinatewise μ-closure of R (μ = the monolith).
6. μ is "abelian."

Con $\mathbb{A}$ =

Centrality and the commutator

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

There is a relation "α centralizes β" on congruences.

$[\alpha, \beta] = 0 \quad \iff \quad \alpha$ centralizes β.

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

For all β there is a largest α such that $[\alpha, \beta] = 0$.

This largest α is denoted $(0 : \beta)$ and called the <u>annihilator</u> of β.

Examples:

1. $\mathbb{Z}_p^{aff}$: monolith $= 1$, $\quad [1, 1] = 0$, $\quad (0 : 1) = 1$.
2. $\mathbb{S}_3^{aff}$: monolith $= \mu$, $\quad [\mu, \mu] = 0$, $\quad (0 : \mu) = \mu$.
3. $\mathbb{SL}(2, 5)^{aff}$: monolith $= \mu$, $\quad [\mu, \mu] = 0$, $\quad (0 : \mu) = 1$.

Theorem (comb. of Kearnes & Szendrei and Freese & McKenzie)

Suppose $\mathbb{A}_1, \ldots, \mathbb{A}_n$ are finite algebras in an idempotent congruence modular variety with $n \geq 3$. Assume $R \leq_{sd} \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$ and R is critical and fork-free, and let R^* be its unique upper cover.

1. Each $\mathbb{A}_i$ is subdirectly irreducible with abelian monolith μ_i.
2. R^* is the $\mu_1 \times \cdots \times \mu_n$-closure of R.
3. $\mathbb{A}_i/(0 : \mu_i) \cong \mathbb{A}_j/(0 : \mu_j)$ for all i, j.
4. There exists a prime p such that each μ_i-class (for any i) has size a power of p.
5. If $(0 : \mu_i) = 1$ for some (equivalently all) i, then:
    1. All μ_i-classes (for all i) have the same fixed size p^k.
    2. Each μ_i-class can be identified with a k-dimensional vector space over $\mathbb{Z}_p$, and with respect to these identifications, R restricted to any strand encodes k linear equations over $\mathbb{Z}_p$.
    3. Let $\mathbb{A}_1(\mu_1) = \mu_1$ considered as a subalgebra of $\mathbb{A}_1 \times \mathbb{A}_1$. There exists a simple affine algebra $\mathbb{M}$ with $|M| = p^k$, and a surjective homomorphism $\mathbb{A}_1(\mu_1) \to \mathbb{M}$ such that 0_{A_1} is a kernel-class.

Almost the same thing can be proved in Taylor varieties.

Theorem (TCT + last-minute help from Keith (thanks!))

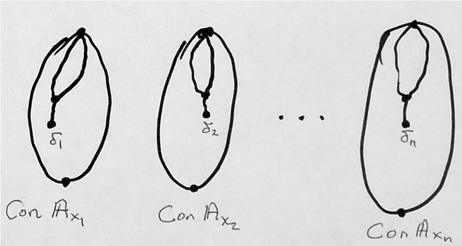
Suppose $\mathbb{A}_1, \ldots, \mathbb{A}_n$ are finite algebras in an (idempotent) Taylor variety with $n \geq 3$. Assume $R \leq_{sd} \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$ and R is critical and fork-free, and let R^* be its unique upper cover.

1. Each $\mathbb{A}_i$ is subdirectly irreducible with abelian monolith μ_i.
2. R^* is the $\mu_1 \times \cdots \times \mu_n$-closure of R.
3. $\mathbb{A}_i/(0 : \mu_i) \cong \mathbb{A}_j/(0 : \mu_j)$ for all i, j.
4. There exists a prime p such that each μ_i-class (for any i) has size a power of p.
5. If $(0 : \mu_i) = 1$ for some (equivalently all) i, then:
    1. ~~All μ_i-classes (for all i) have the same fixed size p^k.~~
    2. Coordinatization? (Conjecture: something nice is true.)
    3. There exists a simple affine algebra $\mathbb{M}$ with $|M| = p^m$, and a surjective homomorphism $\mathbb{A}_1(\mu_1) \to \mathbb{M}$, such that 0_{A_1} is a kernel-class.

Added May 24: see Lecture 3 for an improved statement.

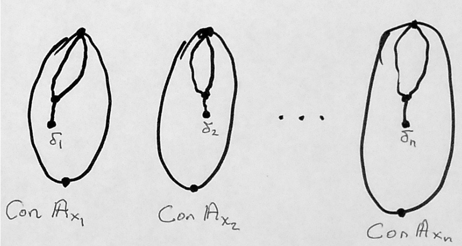
Relativizing to quotients

Suppose $\mathbb{A}_1, \ldots, \mathbb{A}_n$ are finite algebras, and for each i we have a meet-irreducible congruence $\delta_i \in \operatorname{Con} \mathbb{A}_i$.



For each i let $\overline{\mathbb{A}}_i = \mathbb{A}_i/\delta_i$. $\quad \overline{\mathbb{A}}_i$ is SI.

Every $\overline{R} \leq \overline{\mathbb{A}}_1 \times \cdots \times \overline{\mathbb{A}}_n$ naturally pulls back to a $\delta_1 \times \cdots \times \delta_n$-closed relation $R \leq \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$. $\quad$ (R can "encode" whatever $\overline{R}$ encodes.)



$\overline{\mathbb{A}}_i = \mathbb{A}_i/\delta_i$.

$\overline{R} \leq \overline{\mathbb{A}}_1 \times \cdots \times \overline{\mathbb{A}}_n$. $\quad R \leq \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$ is the natural pull-back.

Observe that:

If $\overline{R}$ is ...	then	R is ...
subdirect		subdirect
critical		critical
fork-free		rectangular

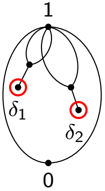
(When R is rectangular, the δ_i and fork-free $\overline{R}$ are uniquely determined.)

Take-away: the last two theorems have versions relativized to meet-irreducible congruences; "fork-free" is replaced by "rectangular."

Similarity

Suppose, in some CSP instance, we have a variable x whose potato has more than one meet-irreducible congruence.

$\mathrm{Con}\,\mathbb{A}_x =$



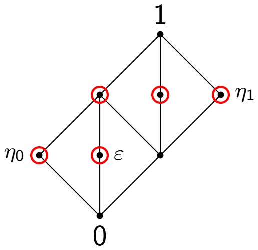
If we have two constraints $R(x, y_1, z_1), R'(x, y_2, z_2)$ (as in the theorem) both mentioning x, then their corresponding congruences $\delta_x^R, \delta_x^{R'}$ at the coordinate x may be the same or different.

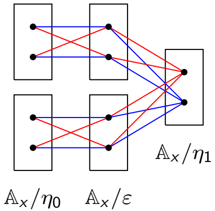
1. If $\delta_x^R = \delta_x^{R'}$, then the linear equations encoded by the two constraints are both defined on the same quotient of $\mathbb{A}_x$ (so are "connected").
2. What if $\delta_x^R \neq \delta_x^{R'}$?

For example, suppose $\mathbb{A}_x = (\mathbb{Z}_4 \times \mathbb{Z}_2)^{aff}$.

Con $\mathbb{A}_x$ "forces" linear dependencies between any triple of incomparable SI quotients.

Con $\mathbb{A}_x$ =





In congruence modular varieties, this is explained via the relation of similarity on SIs. (Freese, Freese & McKenzie).

There is a version of similarity applicable to finite SIs in Taylor varieties (Zhuk). (See Lecture 3.)