Instances of the Constraint Satisfaction Problem in Universal Algebra

Libor Barto

Department of Mathematics and Statistics
McMaster University
Hamilton, ON, Canada
and
Department of Algebra
Charles University
Prague, Czech Republic

OAL 2.0, Kraków, June 2011

CSP and UA

Fruitful cooperation UA $\leftrightarrow$ Computer Science:

- Applications of UA to the complexity of the CSP (not in this lecture)
- Study of the CSP has a great impact on (parts of) UA
  - Surprisingly strong properties of quite general classes of algebras
  - New important classes of algebras discovered (FS - few subpowers, CS - congruence singular)
  - Fundamental new results about classic classes (CP - congruence permutable, CD - congruence distributive)
  - $\Rightarrow$ CSP is not just a fashion

Outline

- Apologies
- Picture of a naked mathematician
- Instance of the CSP
- Examples - CSP in UA

$$\begin{array}{ccccccccc} CS & \rightarrow & CP & \rightarrow & FS & \rightarrow & CM & \rightarrow & Taylor \\ & & & & \uparrow & & \uparrow & & \uparrow \\ & & & & NU & \rightarrow & CD & \rightarrow & CSD(\wedge) \end{array}$$

- Useful technique - absorbing subalgebras (+ some news)

Picture of a naked mathematician

File "naked_george_mcnulty.jpg" not found.

CSP for universal algebraist

Definition

$\mathbf{A}$ ... finite idempotent algebra (always)

Instance of $\mathrm{CSP}(\mathbf{A})$ = finite set V + set $\mathcal{C}$ of constraints

Constraint = subalgebra of $\mathbf{A}^I$, where $I \subseteq V$ is the scope

Solution of the instance = mapping $f : V \to A$ such that $f_{|I} \in R_{|I}$ for every constraint $R \leq \mathbf{A}^I$

Example

every scope is equal to V

$\Downarrow$

set of solutions = intersection of constraints

to study CSP = to study intersection properties of subpowers

Example 1: Taylor algebras

A is Taylor, if

HSP(**A**) (equivalently HS(**A**) ?Szendrei, ?Bulatov) doesn't contain a two-element algebra whose every operation is a projection

$\Leftrightarrow$ HSP(**A**) satisfies a nontrivial Maltsev condition

$\Leftrightarrow$ **A** has a Taylor term Taylor 77, i.e. a term t satisfying a set of identities in two variables x, y of the form

$$\begin{gathered} t(x, \cdot, \cdot, \dots) \approx t(y, \cdot, \cdot, \dots) \\ t(\cdot, x, \cdot, \dots) \approx t(\cdot, y, \cdot, \dots) \\ \dots \\ t(\cdot, \cdot, \dots, x) \approx t(\cdot, \cdot, \dots, y) \end{gathered}$$

$\Leftrightarrow$ HSP(**A**) omits **1** Hobby, McKenzie 88

$\Leftrightarrow$ ...

Smooth theorem (Barto, Kozik, Niven 08)

Let $\mathbf{A}$ *be a Taylor algebra,* $R \leq \mathbf{A}^2$ *subdirect and assume that* $\exists\ k, l \in \mathbb{N}$ *such that* $(R^k \circ R^{-k})^l = A^2$*. Then* $\exists\ a \in A \quad (a, a) \in R$*.*

Corollary (Siggers, Kearnes, Marković, McKenzie 10)

$\mathbf{A}$ *is Taylor iff* $\mathbf{A}$ *has a term* t *satisfying* $t(x, y, y, z) = t(y, z, x, x)$*.*

Proof.

$\mathbf{F}$ ... free algebra on $\{x, y, z\}$
R ... subalgebra of $\mathbf{F}^2$ generated by $(x, y), (y, z), (y, x), (z, x)$.
Apply the theorem $\square$

Other intersection property
(a generalization of Maróti, McKenzie 06):

Theorem (Barto, Kozik 09)

Let $\mathbf{A}$ be a Taylor algebra, p a prime, $p > |A|$, and $\emptyset \neq R \leq \mathbf{A}^p$. If R is invariant under cyclic shift of coordinates, then
$\exists\ a \in A \ \ (a, a, \ldots, a) \in R$.

Corollary

Let $\mathbf{A}$ be an algebra, p a prime, $p > |A|$. Then $\mathbf{A}$ is Taylor iff $\mathbf{A}$ has a cyclic term of arity p
(i.e. a term satisfying $t(x_1, \ldots, x_p) = t(x_2, \ldots, x_p, x_1)$)

Other intersection property
(a generalization of Maróti, McKenzie 06):

Theorem (Barto, Kozik 09)

Let $\mathbf{A}$ be a Taylor algebra, p a prime, $p > |A|$, and $\emptyset \neq R \leq \mathbf{A}^p$. If R is invariant under cyclic shift of coordinates, then
$\exists\ a \in A \ \ (a, a, \ldots, a) \in R$.

Problem

Find a common generalization of this theorem and the smooth theorem.

Reading: L. Barto, M. Kozik: Absorbing subalgebras, cyclic terms and the constraint satisfaction problem

A is $\mathrm{CSD}(\wedge)$, if
HSP(**A**) (or HS(**A**)) doesn't contain a reduct of a module
$\Leftrightarrow$ HSP(**A**) is meet semi-distributive

$$\alpha \wedge \beta = \alpha \wedge \gamma \Rightarrow \alpha \wedge (\beta \vee \gamma) = \alpha \wedge \beta$$

$\Leftrightarrow$ HSP(**A**) omits $\mathbf{1}, \mathbf{2}$

$\Leftrightarrow$ **A** has Willard terms

Definition

An instance of $\mathrm{CSP}(\mathbf{A})$ is $(2,3)$-minimal, if

- $\forall$ three-element $I \subseteq V$ $\exists R \subseteq \mathbf{A}^K$ in $\mathcal{C}$ such that $I \subseteq K$
- $\forall$ at most two-element $I \subseteq V$ $\forall R \subseteq \mathbf{A}^K$, $R' \subseteq \mathbf{A}^{K'}$ such that $I \subseteq K, K'$ we have $R_{|I} = R'_{|I}$

Example 2: $\mathrm{CSD}(\wedge)$ algebras 2/3

Theorem (Barto, Kozik 09 Bulatov 09)

$\mathbf{A}$ *is* $\mathrm{CSD}(\wedge)$ *iff every* $(2,3)$*-minimal instance of* $\mathrm{CSP}(\mathbf{A})$ *has a solution*

Corollary

If $\mathbf{A}$ *is* $\mathrm{CSD}(\wedge)$ *and* $R_1, \ldots, R_n \leq \mathbf{A}^n$ *have the same binary projections, then* $\cap R_i \neq \emptyset$

Example 2: $\mathrm{CSD}(\wedge)$ algebras 3/3

WNU = operation f satisfying
$f(x,\dots,x,y) = f(x,\dots,x,y,x) = \cdots = f(y,x,\dots,x)$

Corollary (Kozik, Valeriote)

A *is* $\mathrm{CSD}(\wedge)$ *iff* **A** *has WNUs of all arities* ≥ 3.

Proof.

Take V big enough. Let $\mathbf{F}$ = free algebra in HSP($\mathbf{A}$) over $\{x,y\}$.
for every three element I we include one constraint $R_I \leq \mathbf{F}^I$, where

$$R_I = \langle (x,x,y),(x,y,x),(y,x,x)\rangle$$

It is $(2,3)$-minimal instance of $\mathrm{CSP}(\mathbf{F}) \Rightarrow \exists$ solution $f : V \to F$.
V is big $\Rightarrow \exists i,j,k\ f(i) = f(j) = f(k) = b$
$b \in R_{\{i,j,k\}} \Rightarrow$ **A** has WNU of arity 3 □

Reading: Doesn't exist yet :(
Collapses of Maltsev conditions for finite algebras

$\mathbb{A}$ ... relational structure (on a finite set A)
Pol($\mathbb{A}$) ... clone of all operations compatible with all relations in $\mathbb{A}$

Theorem (Geiger, Bodnarchuk, Kaluznin, Kotov, Romov 68)

$\forall$ *finite algebra* $\mathbf{A}$ $\exists$ $\mathbb{A}$ *such that* $\mathrm{Pol}(\mathbb{A}) = \mathrm{Clo}(\mathbf{A})$

Definition

Finite $\mathbf{A}$ is finitely related, if $\exists$ $\mathbb{A}$ with finitely many relations such that $\mathrm{Pol}(\mathbb{A}) = \mathrm{Clo}(\mathbf{A})$

Example

Algebras with near-unanimity term (by Baker-Pixley)

(Recall: near-unanimity = operation f satisfying
$x = f(x, \ldots, x, y) = f(x, \ldots, x, y, x) = \cdots = f(y, x, \ldots, x)$)

Example 3: CD $\Rightarrow$ NU 2/2

Theorem (Barto 09)

If $\mathbf{A}$ *is finitely related and* $\mathrm{HSP}(\mathbf{A})$ *is congruence distributive, then* $\mathbf{A}$ *has a near-unanimity term.*

Proof.

Say $\mathbb{A}$ has at most k-ary relations, $\mathrm{Clo}(\mathbf{A}) = \mathrm{Pol}(\mathbb{A})$.

n ... big enough natural number

$V = A^n$

$F \leq \mathbf{A}^V$ ... free algebra on n-generators (=n-ary operations)

For every at most k-element $I \subseteq V$ we include the constraint $F_{|I}$

Solutions of this instance = n-ary operations of $\mathbf{A}$

.... □

Reading: L. Barto: Finitely related algebras in congruence distributive varieties have near unanimity terms

More collapses of Maltsev conditions for finitely related algebras

$\mathbf{A}$ has few subpowers, if $|\{R \leq \mathbf{A}^n\}| \leq 2^{polynomial(n)}$
$\Leftrightarrow$ subpowers of $\mathbf{A}$ have small generating sets
$\Leftrightarrow$ $\mathbf{A}$ has a cube term $\Leftrightarrow$ ...

Example

Maltsev algebras, algebras with near-unanimity operation
Few subpowers $\Rightarrow$ HSP($\mathbf{A}$) is congruence modular

Theorem (Aichinger, Mayr, McKenzie 09)

Every finite algebra with few subpowers is finitely related.

Proof.

Use compact representations of subpowers developed for CSP by Dalmau, Bulatov; Berman, Idziak, Markovic, McKenzie, Valeriote, Willard

. . . . $\square$

Example 4: few subpowers ⇒ finitely related 2/2

Corollary

On a finite set, there is countably many clones with few subpowers (in particular, there is countably many Maltsev clones on a finite set).

(2 years ago open for expansions of $\mathbb{Z}_8$!)

Conjecture (Valeriote's conjecture, Edinburgh conjecture)

If $\mathbf{A}$ is finitely related and HSP($\mathbf{A}$) is congruence modular, then $\mathbf{A}$ has few subpowers.

Reading: A. Bulatov, V. Dalmau: A simple algorithm for Mal'tsev constraints

J. Berman, P. Idziak, P. Markovic, R. McKenzie, M. Valeriote and R. Willard: Varieties with few subalgebras of powers

E. Aichinger, P. Mayr, R. McKenzie: On the number of finite algebraic structures

Example 5: CS - congruence singularity (unfinished)

Congruence uniform .... $|x/\alpha| = |y/\alpha|$

Congruence singular .... $|x/\alpha||x/\beta| = |x/\alpha \vee \beta||x/\alpha \wedge \beta|$

strong malcev conditions....

Bulatov, Dalmau....

Reading: M. Dyer, D. Richerby: An effective dichotomy for the counting constraint satisfaction problem

Definition

B is an *absorbing subuniverse* of an algebra $\mathbf{A}$, if

- $B \leq \mathbf{A}$
- $\mathbf{A}$ has a term t such that $t(a_1, \ldots, a_n) \in B$ whenever all but (at most) 1 of the a_i's are in B.

Example

Singletons are absorbing subuniverses iff $\mathbf{A}$ has a near-unanimity operation

Useful because:

- Algebras often have proper absorbing subuniverses
- Some connectivity properties of subpowers can be pushed inside absorbing subuniverses

Theorem

Let $\mathbf{A}$ be a Taylor algebra, $R \leq \mathbf{A}^2$ subdirect and assume that $\exists\ l \in \mathbb{N}$ such that $(R \circ R^{-1})^l = A^2$ and $R^l = A^2$. Then $\exists\ a \in A$ $(a, a) \in R$.

Proof.

(0) Assume $|A| > 1$

(1) Find a proper absorbing subuniverse B of $\mathbf{A}$

(2) Walk with B to find a proper absorbing subuniverse C of $\mathbf{A}$ such that $S \leq \mathbf{C}^2$ is subdirect, where $S = R \cap C^2$

(3) Prove that $(S \circ S^{-1})^{l'} = A^2$ and $S^{l'} = A^2$

□

Proof.

(0) Assume $|A| > 1$

(1) Find a proper absorbing subuniverse B of $\mathbf{A}$

(2) Walk with B to find a proper absorbing subuniverse C of $\mathbf{A}$ such that $S \leq \mathbf{C}^2$ is subdirect, where $S = R \cap C^2$

(3) Prove that $(S \circ S^{-1})^{l'} = A^2$ and $S^{l'} = A^2$

□

Ad (1):

(Special case of) Absorption Theorem

Let $\mathbf{A}$ be a Taylor algebra, $R \leq \mathbf{A}^2$ subdirect, $R \neq A^2$, and $(R \circ R^{-1})^l = A^2$ for some l. Then $\mathbf{A}$ has a proper absorbing set.

Studying CSPs in NL.....

Theorem (Barto, Kozik, Willard 11)

Let $\mathbf{A}$ be an algebra (no assumptions on $\mathbf{A}$!). Then there exists $a \in A$ such that for any $n \in \mathbb{N}$ and any $B \leq C \leq \mathbf{A}^n$ such that

B is subdirect in $\mathbf{A}^n$

C contains all constant tuples

B absorbs C

we have $(a, a, \ldots, a) \in B$

Ross has a problem

Let $Ab(\mathbf{A})$ be the set of all such a's. Easy to see that $Ab(\mathbf{A}) \leq \mathbf{A}$. What is this??????? (what is it good for? what characterizes this subalgebra? ....)

Problem

Is the following problem decidable? Input is a finite algebra $\mathbf{A}$ *and a subset. Question is whether the subset is an absorbing subuniverse of* $\mathbf{A}$.

Affirmative answer would generalize Maróti's result that NU is decidable

Problem

Is the following problem decidable? Input is a finite relational structure $\mathbb{A}$ *and a subset. Question is weather the subset is an absorbing subuniverse of* $\mathrm{Pol}(\mathbb{A})$.