Posets, graphs and algebras: a case study for the fine-grained complexity of CSP's

Part 2a: Preliminaries on Algebra and Statement of the Conjectures
Part 2b: Some Evidence: General Results

Benoit Larose [1] [2]

[1]Department of Mathematics and Statistics
Concordia University, Montréal

[2]Department of Mathematics
Champlain Regional College, St-Lambert

SSAOS, Slovakia, September 2009

Recap of Talk 1

CSP(**H**)	*complete*	*expressible in*	*NOT expressible in*
NAE SAT	$\mathcal{NP}$	-	Datalog
linear equations	$mod_p\mathcal{L}$	??	Datalog
Horn SAT	$\mathcal{P}$	Datalog	Lin. Datalog
Directed Reach.	$\mathcal{NL}$	Lin. Datalog	Symm. Datalog
Undir. Reach.	$\mathcal{L}$	Symm. Datalog	FO

Overview of Part 2a

- to every CSP is associated an idempotent algebra $\mathbb{A}$;
- the identities satisfied by this algebra give lower bounds on the complexity of the CSP;
- conjecturally, the identities capture the complexity of the CSP.

A Fundamental Duality

Let A be a finite set.

- Let $f : A^n \to A$ be an *n-ary operation* on A;
- Let $\theta \subseteq A^k$ be a *k-ary relation* on A.
- The operation f *preserves* the relation θ, or θ is *invariant* under f, if the following holds:

$$\underbrace{\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \cdots & \vdots \\ a_{k,1} & \cdots & a_{k,n} \end{bmatrix}}_{\text{columns in } \theta} \overset{f}{\longmapsto} \underbrace{\begin{bmatrix} b_1 \\ \vdots \\ b_k \end{bmatrix}}_{\theta}$$

Applying f to the rows of the matrix with columns in θ yields a tuple of θ.

A Fundamental Duality, cont'd

Example

On $\{0,1\}$ let $\leq$ denote the usual ordering $\{(0,0),(0,1),(1,1)\}$.
An operation f preserves $\leq$ iff it is *monotonic*, i.e.
$f(x_1,\dots,x_n) \leq f(y_1,\dots,y_n)$ whenever $x_i \leq y_i$ for all $1 \leq i \leq n$.

$$\begin{bmatrix} x_1 & \cdots & x_n \\ \rotatebox{90}{$\geq$} & \cdots & \rotatebox{90}{$\geq$} \\ y_1 & \cdots & y_n \end{bmatrix} \stackrel{f}{\longmapsto} \begin{bmatrix} f(x_1,\dots,x_n) \\ \rotatebox{90}{$\geq$} \\ f(y_1,\dots,y_n) \end{bmatrix}$$

$\mathbb{A}$lgebras

Let A be a non-void set.

- A (non-indexed) *algebra* is a pair $\mathbb{A} = \langle A; F \rangle$ where F is a set of operations on A, the *basic* or *fundamental* operations of $\mathbb{A}$.
- an operation f is *idempotent* if

$$f(x, \ldots, x) = x \text{ for all } x;$$

  i.e. f is idempotent iff it preserves every one-element unary relation $\{a\}$;
- an algebra is idempotent if all its basic operations are idempotent.

The Algebra $\mathbb{A}(\mathbf{H})$

Let $\mathbf{H} = \langle A; \theta_1, \dots, \theta_r \rangle$ be a relational structure.

The *algebra associated to* $\mathbf{H}$ is

$$\mathbb{A}(\mathbf{H}) = \langle A; F \rangle$$

where $F = Pol(R)$ consists of all idempotent operations on A that preserve every θ_i, i.e. the *polymorphisms of* $R = \{\theta_1, \dots, \theta_r\} \cup \{\{a\} : a \in A\}$.

The Algebra $\mathbb{A}(\mathbf{H})$, cont'd

Example

- Let $\mathbf{H} = \langle \{0,1\}; \leq, \{0\}, \{1\} \rangle$.
- $\mathbb{A}(\mathbf{H}) = \langle \{0,1\}; Pol(\leq, \{0\}, \{1\}) \rangle$.
- The term (basic) operations of $\mathbb{A}(\mathbf{H})$ are all monotonic Boolean operations f such that $f(0,\ldots,0) = 0$ and $f(1,\ldots,1) = 1$.

Varieties

- A *variety* is a class of similar algebras closed under the formation of homomorphic images, subalgebras and products;
- the *variety generated by* $\mathbb{A}$ is the smallest variety $\mathcal{V}(\mathbb{A})$ containing the algebra $\mathbb{A}$;
- (Birkhoff) Varieties $=$ equational classes.

Outline of this section

- we present a lemma correlating the existence of certain “minimal” algebras in $\mathcal{V}(\mathbb{A})$ with the *typeset* of $\mathcal{V}(\mathbb{A})$;
- we describe key properties of these “minimal” algebras, connecting them to the problems described in Talk 1.

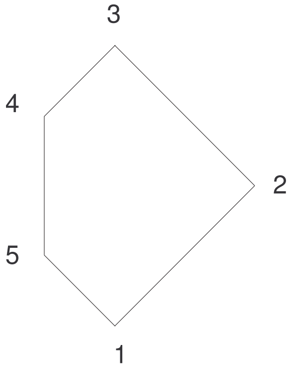
A very vague overview of types

- to each (finite) algebra $\mathbb{A}$ is associated a set of *types*;
- the possible types are:
  - the *unary type*, or type 1;
  - the *affine* type, or type 2;
  - the *Boolean* type, or type 3;
  - the *lattice* type, or type 4;
  - the *semilattice* type, or type 5.
- the *typeset* of the variety $\mathcal{V}(\mathbb{A})$ is the union of all typesets of all finite algebras in it.

The Ordering of Types

we shall refer later to the following ordering of types:

$$1 < 2 < 3 > 4 > 5 > 1$$



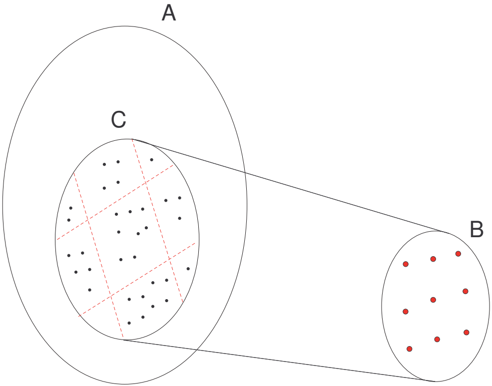
Divisor algebras

Definition (Divisors)

We say that the algebra $\mathbb{B}$ is a *divisor* of the algebra $\mathbb{A}$ if $\mathbb{B} \in HS(\mathbb{A})$, i.e. it is a homomorphic image of a subalgebra of $\mathbb{A}$.

Divisor algebras, cont'd

The algebra $\mathbb{B}$ is a homomorphic image of the subalgebra $\mathbb{C}$ of $\mathbb{A}$, hence $\mathbb{B}$ is a *divisor* of $\mathbb{A}$:



Strictly simple algebras

Definition (Strictly simple algebra)

An algebra is *strictly simple* if it has no divisors other than itself or one-element algebras.

A key lemma

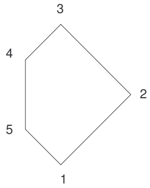
- every strictly simple idempotent algebra has a unique type associated to it;
- The next lemma is one of the two key links between typesets and CSP's we shall require:

Lemma (Valeriote, 2007)

Let $\mathbb{A}$ be an idempotent algebra, and suppose type i is in the typeset of $\mathcal{V}(\mathbb{A})$. Then $\mathbb{A}$ has a strictly simple divisor of type $\leq i$.

Valeriote's Lemma, cont'd

To illustrate:



- $\mathcal{V}(\mathbb{A})$ admits type 1 iff $\mathbb{A}$ has a strictly simple divisor of unary type (type 1);
- if $\mathcal{V}(\mathbb{A})$ omits types 1 and 5 but admits type 4, then $\mathbb{A}$ has a strictly simple divisor of lattice type (type 4);
- Etc.

A property of strictly simple algebras

- We now have conditions on the existence of strictly simple divisors of our algebra $\mathbb{A}$;
- Szendrei (1992) has completely classified these algebras according to their type. We need the following consequences (we split up the result into 4 distinct lemmas):

A property of strictly simple algebras, cont'd

Lemma (unary type 1)

Let $\mathbb{A}$ be a strictly simple idempotent algebra of unary type. Then it is a 2-element algebra, and its basic operations preserve the relation

$$\theta = \{0,1\}^3 \setminus \{(0,0,0),(1,1,1)\}.$$

Lemma (affine type 2)

Let $\mathbb{A}$ be a strictly simple idempotent algebra of affine type. Then there exists an Abelian group structure on A such that the basic operations of $\mathbb{A}$ preserve the relation

$$\mu = \{(x,y,z) : x+y=z\}.$$

A property of strictly simple algebras, cont'd

Lemma (lattice type 4)

Let $\mathbb{A}$ be a strictly simple idempotent algebra of lattice type. Then it is a 2-element algebra, and its basic operations preserve the usual ordering $\leq$ on $\{0, 1\}$.

Lemma (semilattice type 5)

Let $\mathbb{A}$ be a strictly simple idempotent algebra of semilattice type. Then it is isomorphic to a 2-element algebra whose basic operations preserve the relation

$$\rho = \{(x, y, z) : (y \wedge z) \rightarrow x\}.$$

A quick recap:

- From Talk 1:
  - some specific CSP's that are hard for the complexity classes $\mathcal{NP}$, $\mathcal{P}$, $\mathcal{NL}$ and $mod_p\mathcal{L}$;
  - CSP's that are not expressible in Datalog, Linear Datalog and Symmetric Datalog;
- from Talk 2:
  - if the variety generated by the idempotent algebra $\mathbb{A}$ admits type i, then there exists a divisor of $\mathbb{A}$ of type $\leq i$;
  - the basic operations of this divisor preserve specific relations related to the problems described in Talk 1.

Outline of this section

- We describe a lemma that relates the complexity and expressibility of the “divisor CSP” to the CSP associated to the algebra $\mathbb{A}$;
- We deduce hardness and non-expressibility results in terms of the typeset of $\mathcal{V}(\mathbb{A})$;
- we present natural conjectures associated to the above-mentioned results.

A reduction lemma

Lemma (BL, Tesson, 2007)

Let $\mathbf{H}$ *be a core. Let* $\mathbb{B}$ *be a divisor of* $\mathbb{A}(\mathbf{H})$*, and let* $\mathbf{H}'$ *be a structure whose basic relations are irredundant and invariant under the operations of* $\mathbb{B}$*. Then*

- *there is a first-order reduction of* $CSP(\mathbf{H}')$ *to* $CSP(\mathbf{H})$*;*
- *if* $\neg CSP(\mathbf{H})$ *is expressible in (Linear, Symmetric) Datalog then so is* $\neg CSP(\mathbf{H}')$*.*

Hardness results

Corollary (1)

Let $\mathbf{H}$ *be a core, and let* $\mathbb{A} = \mathbb{A}(\mathbf{H})$.

- *(BJK, 2000) If* $\mathcal{V}(\mathbb{A})$ *admits the unary type, then* $CSP(\mathbf{H})$ *is* $\mathcal{NP}$*-complete;*
- *if* $\mathcal{V}(\mathbb{A})$ *admits the affine type, then* $CSP(\mathbf{H})$ *is* $mod_p\mathcal{L}$*-hard* $(\exists p)$*;*
  Otherwise:
- *if* $\mathcal{V}(\mathbb{A})$ *admits the semilattice type, then* $CSP(\mathbf{H})$ *is* $\mathcal{P}$*-hard;*
- *if* $\mathcal{V}(\mathbb{A})$ *admits the lattice type, then* $CSP(\mathbf{H})$ *is* $\mathcal{NL}$*-hard.*

Non-expressibility results

Corollary (2)

Let $\mathbf{H}$ *be a core, and let* $\mathbb{A} = \mathbb{A}(\mathbf{H})$.

- *(BL, Zádori, 2006) If* $\mathcal{V}(\mathbb{A})$ *admits the unary or affine type, then* $\neg CSP(\mathbf{H})$ *is not expressible in Datalog;*
- *if* $\mathcal{V}(\mathbb{A})$ *admits the semilattice type, then* $\neg CSP(\mathbf{H})$ *is not expressible in Linear Datalog;*
- *if* $\mathcal{V}(\mathbb{A})$ *admits the lattice type, then* $\neg CSP(\mathbf{H})$ *is not expressible in Symmetric Datalog.*

Recap

Let $\mathbf{H}$ be a core, and let $\mathbb{A} = \mathbb{A}(\mathbf{H})$.

$\mathcal{V}(\mathbb{A})$		$CSP(\mathbf{H})$	$CSP(\mathbf{H})$
omits	*admits*	*complexity*	*expressibility*
	1	$\mathcal{NP}$-complete	not Datalog
1	2	$mod_p\mathcal{L}$-hard $(\exists p)$	not Datalog
1,2	5	$\mathcal{P}$-hard	not Linear Datalog
1,2,5	4	$\mathcal{NL}$-hard	not Symmetric Datalog

Conjectures

Conjecture

Let $\mathbf{H}$ *be a core, and let* $\mathbb{A} = \mathbb{A}(\mathbf{H})$.

- *(BJK) If* $\mathcal{V}(\mathbb{A})$ *omits type 1 then CSP*$(\mathbf{H})$ *is in* $\mathcal{P}$;
- *(BL, Z)* $\mathcal{V}(\mathbb{A})$ *omits types 1, 2* $\Leftrightarrow \neg$*CSP*$(\mathbf{H})$ *is in Datalog;*
- *(BL, T)* $\mathcal{V}(\mathbb{A})$ *omits types 1, 2, 5* $\Leftrightarrow \neg$*CSP*$(\mathbf{H})$ *is in Linear Datalog;*
- *(BL, T)* $\mathcal{V}(\mathbb{A})$ *omits 1, 2, 4, 5* $\Leftrightarrow \neg$*CSP*$(\mathbf{H})$ *is in Symmetric Datalog.*

Remark: all known CSP's in $\mathcal{NL}$ ($\mathcal{L}$) are in Linear (Symmetric) Datalog.

Some Evidence: General Results

- We present results supporting the conjectures;
- the results are of a general nature, i.e. with no restrictions on the general "shape" of the relational structure **H**;
- in Talk 3, we'll look in detail at some evidence in the case where the target consists of a single binary relation (plus unary relations);

The Boolean Case

$\mathcal{V}(\mathbb{A})$			
omits	*admits*	*complexity*	*in/not in*
	1	**NP**-complete	-/Datalog
1	2	$\oplus$**L**-complete	-/Datalog
1,2	5	**P**-complete	Datalog/Linear
1,2,5	4	**NL**-complete	Linear/Symmetric
1,2,4,5		**L**-complete/FO	Symmetric/-

Preprimal algebras (i.e. maximal clones)

- consider a relational structure $\mathbf{H} = \langle H; \theta_1, \ldots, \theta_r; \{h\}(h \in H)\rangle$ where $Pol(\theta_1, \ldots, \theta_r)$ is a maximal clone M;
- we add the one-element unary relations to ensure we have core structures.
- Rosenberg's celebrated theorem (1970) characterises maximal clones, they fall into 6 classes;
- for all but one class, we can determine the exact descriptive and algorithmic complexity of the CSP (BL, Tesson (2007)) and the conjectures are verified:

Preprimal algebras, cont'd

Let $M = Pol(\rho)$ be a maximal clone.

- E ρ is an equivalence relation: $CSP(\mathbf{H})$ is in symmetric Datalog, and is $\mathcal{L}$-complete.
- C ρ is a central relation: $CSP(\mathbf{H})$ is in symmetric Datalog, and is FO or $\mathcal{L}$-complete.
- R ρ is a regular relation: $CSP(\mathbf{H})$ is $\mathcal{N}P$-complete;
- A ρ is an affine relation: $CSP(\mathbf{H})$ is $mod_p\mathcal{L}$-complete;
- P ρ is the graph of a permutation: $CSP(\mathbf{H})$ is in symmetric Datalog, and is $\mathcal{L}$-complete.
- O ρ is a bounded partial order: see Talk 3.

Evidence for the Algebraic Dichotomy Conjecture

Conjecture

Let $\mathbf{H}$ *be a core, and let* $\mathbb{A} = \mathbb{A}(\mathbf{H})$*.*
If $\mathcal{V}(\mathbb{A})$ *omits type 1 then CSP*$(\mathbf{H})$ *is in* $\mathcal{P}$*.*

- the 3 element case (Bulatov, 2002);
- the conservative case (Bulatov, 2003): every subset of H is a basic relation of the target structure $\mathbf{H}$;
- Few subpowers (Berman, Idziak, Markovic, McKenzie, Valeriote, Willard, 2008): if the associated algebra admits a k-edge term, then the CSP is tractable;
- various special cases (see Talk 3).

Evidence for the Bounded Width Conjecture

Conjecture

Let $\mathbf{H}$ *be a core, and let* $\mathbb{A} = \mathbb{A}(\mathbf{H})$.
$\mathcal{V}(\mathbb{A})$ *omits types 1, 2* $\Leftrightarrow \neg CSP(\mathbf{H})$ *is in Datalog.*

Evidence for the Bounded Width Conjecture

Conjecture

Let $\mathbf{H}$ *be a core, and let* $\mathbb{A} = \mathbb{A}(\mathbf{H})$.
$\mathcal{V}(\mathbb{A})$ *omits types 1, 2* $\Leftrightarrow \neg CSP(\mathbf{H})$ *is in Datalog.*

PROVED !

The Bounded Width Conjecture

- $\neg CSP(\mathbf{H})$ is expressible in Datalog iff it can be solved by "local consistency" methods, i.e. if it admits a complete set of obstructions of bounded treewidth (Feder, Vardi, 98);
- $\neg CSP(\mathbf{H})$ is in (j,k)-Datalog (or has *width* (j,k)) if it recognised by a Datalog program whose rules have at most k variables and with IDB's of arity at most j.

The Bounded Width Conjecture, cont'd

Definition

Let $n \geq 2$. An n-ary idempotent operation w is a *weak near unanimity (NU) operation* if it satisfies the identities

$$w(x, \cdots, x, y) \approx w(x, \cdots, x, y, x) \approx \cdots \approx w(y, x, \cdots, x).$$

Example

- any binary, idempotent, commutative operation is a weak NU;
- on an Abelian group of order n, the operation $x_1 + \cdots + x_{n+1}$ is a weak NU operation.

The Bounded Width Conjecture, cont'd

Theorem (Maróti, McKenzie, 2008)

Let $\mathbb{A}$ be a finite, idempotent algebra.

- $\mathcal{V}(\mathbb{A})$ *omits type 1 iff* $\mathbb{A}$ *has a weak NU term;*
- $\mathcal{V}(\mathbb{A})$ *omits types 1, 2 iff* $\mathbb{A}$ *has weak NU terms of all but finitely many arities.*

The Bounded Width Conjecture, cont'd

Theorem (Barto, Kozik (2009))

Let $\mathbf{H}$ *be a finite relational structure whose basic relations have maximum arity* r*.*
If $\mathbb{A}(\mathbf{H})$ *has weak NU terms of all but finitely many arities, then* $\neg CSP(\mathbf{H})$ *has width* $(2, \max(3, r))$*.*

Some Consequences of the BK Theorem

- it is decidable to determine if a $\neg$ CSP is expressible in Datalog;
- the Datalog hierarchy collapses (IDB's of arity 2 are sufficient in all cases)
- strongly supports the paradigm that the complexity of CSP's is tightly linked to the typeset of the associated algebra;
- $\neg$CSP's of bounded width $=$ $\neg$CSP's solvable by poly-size monotone circuits (BL, Valeriote, Zádori, 2009)
- Etc. (see Talk 3)

The Linear Datalog Conjecture

Conjecture

Let $\mathbf{H}$ *be a core, and let* $\mathbb{A} = \mathbb{A}(\mathbf{H})$.
$\mathcal{V}(\mathbb{A})$ *omits types 1, 2, 5* $\Leftrightarrow \neg CSP(\mathbf{H})$ *is in Linear Datalog.*

The Linear Datalog Conjecture, cont'd

Definition

Let $n \geq 3$. An n-ary idempotent operation w is a *near unanimity (NU) operation* if it satisfies the identities

$$x \approx w(x, \cdots, x, y) \approx w(x, \cdots, x, y, x) \approx \cdots \approx w(y, x, \cdots, x).$$

An NU operation of arity 3 is called a *majority* operation.

Example

The prototypical majority operation on $\{0, \ldots, n-1\}$:
$m(x, y, z) = \max(\min(x, y), \min(x, z), \min(y, z))$.

Evidence for The Linear Datalog Conjecture

- Fact: If $\mathbb{A}$ has an NU term, then $\mathcal{V}(\mathbb{A})$ omits types 1, 2, 5. (since NU implies congruence-distributivity)
- Still open: does NU imply Linear Datalog ?
- Remark: CD $=$ omit 1, 2, 5 $+ \epsilon$
- Remark: CD $+$ finite signature implies NU (Barto) ...

Theorem (Dalmau, Krokhin (2007))

Let $\mathbf{H}$ *be a core, and let* $\mathbb{A} = \mathbb{A}(\mathbf{H})$. *If* $\mathbb{A}$ *has a majority term then* $\neg CSP(\mathbf{H})$ *is in Linear Datalog.*

The Symmetric Datalog Conjecture

Conjecture

Let $\mathbf{H}$ *be a core, and let* $\mathbb{A} = \mathbb{A}(\mathbf{H})$*.*
$\mathcal{V}(\mathbb{A})$ *omits 1, 2, 4, 5* $\Leftrightarrow \neg CSP(\mathbf{H})$ *is in Symmetric Datalog.*

The Symmetric Datalog Conjecture, cont'd

Definition (Hagemann, Mitschke (1973))

Let $n \geq 2$ and let $\mathbb{A}$ be a finite idempotent algebra. The variety $\mathcal{V}(\mathbb{A})$ is *n-permutable* if $\mathbb{A}$ has terms $p_1, \ldots, p_{n-1}$ satisfying the identities

$$
\begin{aligned}
x &\approx p_1(x, y, y) && (1)\\
p_i(x, x, y) &\approx p_{i+1}(x, y, y) \text{ for all } i && (2)\\
p_{n-1}(x, x, y) &\approx y. && (3)
\end{aligned}
$$

The Symmetric Datalog Conjecture, cont'd

- $\mathcal{V}(\mathbb{A})$ is n-permutable for some n iff its typeset is contained in $\{2, 3\}$ (Hobby, McKenzie, 1983);
- hence $\mathcal{V}(\mathbb{A})$ omits types 1, 2, 4, 5 iff $\mathcal{V}(\mathbb{A})$ is n-permutable and omits types 1, 2;
- by the BK theorem, it follows that the conjecture may be restated as follows:

Conjecture

Let $\mathbf{H}$ *be a core, and let* $\mathbb{A} = \mathbb{A}(\mathbf{H})$. *If* $\neg CSP(\mathbf{H})$ *is in Datalog, then*
$\exists\, n\ \mathcal{V}(\mathbb{A})$ *is n-permutable* $\Leftrightarrow \neg CSP(\mathbf{H})$ *is in Symmetric Datalog.*

Maltsev operations

Definition

A 3-ary idempotent operation M is a *Maltsev operation* if it satisfies the identities

$$M(x, y, y) \approx x \approx M(x, y, y).$$

Example

The prototypical Maltsev operation: $M(x, y, z) = xy^{-1}z$ on a group.

- Observe: $\mathcal{V}(\mathbb{A})$ is 2-permutable iff it has a Maltsev term.

More Evidence

Theorem (Dalmau, BL (2008))

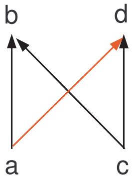
Let $\mathbf{H}$ *be a core and let* $\mathbb{A} = \mathbb{A}(\mathbf{H})$*. If* $\neg CSP(\mathbf{H})$ *is in Datalog and* $\mathcal{V}(\mathbb{A})$ *is 2-permutable, then* $\neg CSP(\mathbf{H})$ *is in symmetric Datalog.*

Sketch:

- 2-permutability implies congruence-modularity;
- CM implies $\mathcal{V}(\mathbb{A})$ omits types 1,5 and has empty tails (HMcK);
- hence $\mathcal{V}(\mathbb{A})$ omits types 1,2,5 and has empty tails so it is congruence-distributive(HMcK);
- hence $\mathcal{V}(\mathbb{A})$ is arithmetical, and admits a majority term (Pixley, 1963);

Sketch, cont'd

- by DK, majority $\Rightarrow \neg CSP(\mathbf{H})$ is in linear Datalog;
- majority implies we can look only at binary relations (Baker-Pixley, 1975));
- binary relations invariant under a Maltsev operation are "rectangular": this allows us to "symmetrise" the linear Datalog program.



More Evidence

- strictly simple algebras of type 3: in Symmetric Datalog (Egri, BL, Tesson, 2007)
- algebras term equivalent to algebras of CSP's in FO: in Symmetric Datalog (E,BL,T)
- various special cases (see Talk 3)

Recap of Talk 2

- to each CSP we associate an idempotent algebra $\mathbb{A}$;
- we conjecture that the typeset of $\mathcal{V}(\mathbb{A})$ "controls" the (descriptive and algorithmic) complexity of $CSP(\mathbf{H})$;
- there is some good evidence supporting these conjectures.

Outline of Talk 3

- CSP's based on target structures with binary relations:
- sufficient to prove the Dichotomy Conjecture (FV 93)
- may use techniques from graph theory;
- posets and reflexive digraphs: topological methods also;
- complete classification in the cases of:
  - list homomorphisms of graphs;
  - series-parallel posets.