Algorithms in Universal Algebra and the UACalculator

Ralph Freese

University of Hawaii

June 2010

UACalc Web Site:
http://uacalc.org/

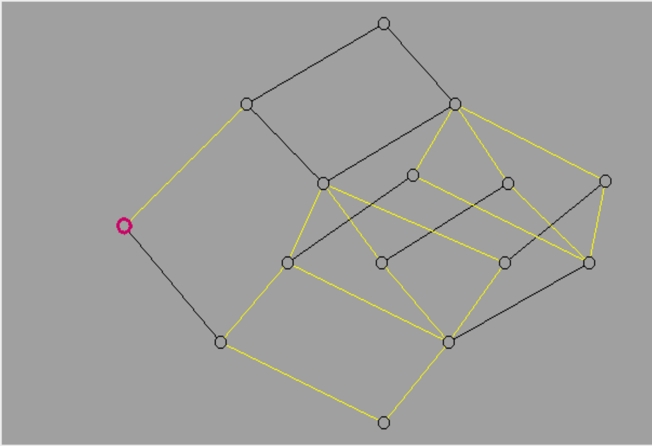
File Edit HSP Tasks Maltsev Drawing Help

Editor | Algebras | Computations | Con | Sub | Drawing

idx	JI	MI	...	...	...	...	elem
0	☐	☐					|0|1|2|3|4|5|6|
1	☑	☐	2				|0|1|2,3|4|5,6|
2	☑	☐	2				|0|1,4|2|3|5|6|
3	☑	☐	2				|0|1,4|2,6|3,5|
4	☑	☐	2				|0|1,4|2,5|3,6|
5	☐	☐					|0|1,4|2,3|5,6|
6	☑	☐	5				|0,1,4|2|3|5|6|
7	☑	☑	5				|0|1,2,3|4,5,6|
8	☐	☑					|0,1,4|2,6|3,5|
9	☐	☑					|0,1,4|2,5|3,6|
10	☐	☑					|0,1,4|2,3|5,6|
11	☐	☐					|0|1,4|2,3,5,6|
12	☐	☑					|0|1,2,3,4,5,6|
13	☐	☑					|0,1,4|2,3,5,6|
14	☐	☐					|0,1,2,3,4,5,6|

Labels Dragging Improve Speed

> < ↻ >< <> ++ ◯ JI ◯ L C ◯ Id ◯ J D ◉ Off ◯ MI ◯ U C ◯ Fil



Algebras

Internal	Name	Type	Description	File
A0	z3_2.alg	BASIC		z3_2.xml
A1	QuotOfz3_2.alg	QUOTIENT	The quotient of z3_2.alg by |0,1,2|3|4|5|6|7|8|	

Hard Tasks

Tasks Menu:

- Free Algebra
- **B** in $\boldsymbol{V}(\mathbf{A})$
- Sub Power
- Primality

Hard Tasks

Tasks Menu:

- Free Algebra
- **B** in $\boldsymbol{V}(\mathbf{A})$
- Sub Power
- Primality

Maltsev Menu:

- Distributivity (Jónsson terms)
- Modularity (Gumm terms)
- *n*-Permutability (Hagemann-Mitschke terms)
- Maltsev term
- Majority term
- Pixley term
- near unamimity term
- Siggers Taylor term

Hard Tasks

Theorem (Freese & Valeriote)

The following problems are EXPTIME complete: Given a finite algebra $\mathbf{A}$*,*

Hard Tasks

Theorem (Freese & Valeriote)

The following problems are EXPTIME complete: Given a finite algebra $\mathbf{A}$,

- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence modular?*

Hard Tasks

Theorem (Freese & Valeriote)

The following problems are EXPTIME complete: Given a finite algebra $\mathbf{A}$*,*

- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence modular?*
- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence distributive?*

Hard Tasks

Theorem (Freese & Valeriote)

The following problems are EXPTIME complete: Given a finite algebra $\mathbf{A}$*,*

- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence modular?*
- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence distributive?*
- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence semidistributive?*

Hard Tasks

Theorem (Freese & Valeriote)

The following problems are EXPTIME complete: Given a finite algebra $\mathbf{A}$*,*

- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence modular?*
- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence distributive?*
- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence semidistributive?*
- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence meet semidistributive?*

Hard Tasks

Theorem (Freese & Valeriote)

The following problems are EXPTIME complete: Given a finite algebra $\mathbf{A}$*,*

- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence modular?*
- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence distributive?*
- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence semidistributive?*
- *Is* $\boldsymbol{V}(\mathbf{A})$ *congruence meet semidistributive?*
- *Does* $\mathbf{A}$ *have a Taylor term?*

Hard Tasks

Theorem (Freese & Valeriote)

The following problems are EXPTIME complete: Given a finite algebra $\mathbf{A}$*,*

- *Is* $\mathbf{V}(\mathbf{A})$ *congruence modular?*
- *Is* $\mathbf{V}(\mathbf{A})$ *congruence distributive?*
- *Is* $\mathbf{V}(\mathbf{A})$ *congruence semidistributive?*
- *Is* $\mathbf{V}(\mathbf{A})$ *congruence meet semidistributive?*
- *Does* $\mathbf{A}$ *have a Taylor term?*
- *Does* $\mathbf{A}$ *have a Hobby-McKenzie term?*

Results

Desc: Finding Jonsson terms for A4 (Baker2)

Index	Term
0	x
1	bak(x,y,z)
2	bak(x,z,z)
3	bak(z,x,y)
4	z

Tasks

	Description	Pass	Pass Size	Size	Time Left Pass	Time Next Pass	Status
	F(5) over A0 (lyndon)	4	326	326		0	DONE
	Test if A2 in V(A3)	3	476	528			DONE
->	Finding Jonsson terms for A4 (B...	2	10	10			DONE
	F(4) over A6 (n5)	4	321556	662106	208:52:22	676:37:50	CANCE
	F(4) over A5 (m3)	4	15072	19982	2:57	5:28	RUNNII

```
finding Jonsson terms
  Looking for a Day quadruple in A^2
    There are no Day quadruples in the subalgebras of A^2.
  So this algebra lies in a CM variety.  (0 ms)
  constructing free algebra on 2 generators over Baker2
    using subdirect decompositions to eliminate some projections.
    number of projections: 2, sizes: 2(2),   (0 ms)
    subpower closing ...
      pass: 0, size: 2
```

$\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

Problem

(McNulty) How hard is this.

$\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

Problem

(McNulty) How hard is this.
With **A** *fixed (the membership problem).*

$\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

Problem

(McNulty) How hard is this.
With **A** *fixed (the membership problem).*
With neither fixed (the universal membership problem).

$\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

Problem

(McNulty) How hard is this.
With **A** *fixed (the membership problem).*
With neither fixed (the universal membership problem).

- *Both are in 2EXPTIME.*

$\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

Problem

(McNulty) How hard is this.
With **A** *fixed (the membership problem).*
With neither fixed (the universal membership problem).

- *Both are in 2EXPTIME.*
- *If* **A** *is finitely based, the membership problem is polynomial time.*

$\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

Problem

(McNulty) How hard is this.
With $\mathbf{A}$ *fixed (the membership problem).*
With neither fixed (the universal membership problem).

- *Both are in 2EXPTIME.*
- *If* $\mathbf{A}$ *is finitely based, the membership problem is polynomial time.*
- *(Jackson & McNulty) The membership problem for Lyndon's algebra, is polynomial time.*

$\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

Problem

(McNulty) How hard is this.
With **A** *fixed (the membership problem).*
With neither fixed (the universal membership problem).

- *Both are in 2EXPTIME.*
- *If* **A** *is finitely based, the membership problem is polynomial time.*
- *(Jackson & McNulty) The membership problem for Lyndon's algebra, is polynomial time.*
- *(Székely) There is an* **A** *where it is NP-complete.*

$\mathbf{B} \in V(\mathbf{A})$

Problem

(McNulty) How hard is this.
With **A** *fixed (the membership problem).*
With neither fixed (the universal membership problem).

- *Both are in 2EXPTIME.*
- *If* **A** *is finitely based, the membership problem is polynomial time.*
- *(Jackson & McNulty) The membership problem for Lyndon's algebra, is polynomial time.*
- *(Székely) There is an* **A** *where it is NP-complete.*
- *(Kozik & Kun) There is a groupoid where it's NP-complete.*

$\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

Problem

(McNulty) How hard is this.
With **A** *fixed (the membership problem).*
With neither fixed (the universal membership problem).

- *Both are in 2EXPTIME.*
- *If* **A** *is finitely based, the membership problem is polynomial time.*
- *(Jackson & McNulty) The membership problem for Lyndon's algebra, is polynomial time.*
- *(Székely) There is an* **A** *where it is NP-complete.*
- *(Kozik & Kun) There is a groupoid where it's NP-complete.*
- *(Jackson & McKenzie) There is a semigroup where it's NP-complete.*

$\mathbf{B} \in V(\mathbf{A})$

Problem

(McNulty) How hard is this.
With **A** *fixed (the membership problem).*
With neither fixed (the universal membership problem).

- *Both are in 2EXPTIME.*
- *If* **A** *is finitely based, the membership problem is polynomial time.*
- *(Jackson & McNulty) The membership problem for Lyndon's algebra, is polynomial time.*
- *(Székely) There is an* **A** *where it is NP-complete.*
- *(Kozik & Kun) There is a groupoid where it's NP-complete.*
- *(Jackson & McKenzie) There is a semigroup where it's NP-complete.*
- *(Kozik) There is an* **A** *where it is PSPACE-complete.*

$\mathbf{B} \in V(\mathbf{A})$

Problem

(McNulty) How hard is this.
*With **A** fixed (the membership problem).*
With neither fixed (the universal membership problem).

- *Both are in 2EXPTIME.*
- *If **A** is finitely based, the membership problem is polynomial time.*
- *(Jackson & McNulty) The membership problem for Lyndon's algebra, is polynomial time.*
- *(Székely) There is an **A** where it is NP-complete.*
- *(Kozik & Kun) There is a groupoid where it's NP-complete.*
- *(Jackson & McKenzie) There is a semigroup where it's NP-complete.*
- *(Kozik) There is an **A** where it is PSPACE-complete.*
- *(Kozik) There is an **A** where it is 2EXPTIME-complete.*

Directoids: Ježek and Quackenbush

A **directoid** is a groupoid defined on a p. o. set such that

$$x \leq xy \qquad y \leq xy \qquad x \leq y \implies xy = yx = y$$

Directoids: Ježek and Quackenbush

A **directoid** is a groupoid defined on a p. o. set such that

$$x \leq xy \qquad y \leq xy \qquad x \leq y \implies xy = yx = y$$

It is an equational class:

$$x^2 \approx x \quad (xy)x \approx xy \quad y(xy) \approx xy \quad x((xy)z) \approx (xy)z$$

Directoids: Ježek and Quackenbush

A **directoid** is a groupoid defined on a p. o. set such that

$$x \leq xy \qquad y \leq xy \qquad x \leq y \implies xy = yx = y$$

It is an equational class:

$$x^2 \approx x \quad (xy)x \approx xy \quad y(xy) \approx xy \quad x((xy)z) \approx (xy)z$$

- Is every finite directoid finitely based?

Directoids: Ježek and Quackenbush

A **directoid** is a groupoid defined on a p. o. set such that

$$x \leq xy \qquad y \leq xy \qquad x \leq y \implies xy = yx = y$$

It is an equational class:

$$x^2 \approx x \quad (xy)x \approx xy \quad y(xy) \approx xy \quad x((xy)z) \approx (xy)z$$

- Is every finite directoid finitely based?
- Hajilarov gave a 6 element directoid, **H**, which he asserted is INFB:

Directoids: Ježek and Quackenbush

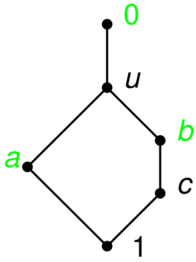
A **directoid** is a groupoid defined on a p. o. set such that

$$x \leq xy \qquad y \leq xy \qquad x \leq y \implies xy = yx = y$$

It is an equational class:

$$x^2 \approx x \quad (xy)x \approx xy \quad y(xy) \approx xy \quad x((xy)z) \approx (xy)z$$

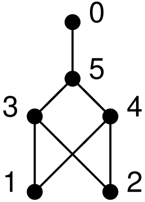
- Is every finite directoid finitely based?
- Hajilarov gave a 6 element directoid, **H**, which he asserted is INFB:



$\cdot$	1	a	b	c	u	0
1	1	a	b	c	u	0
a	a	a	0	u	u	0
b	b	0	b	b	u	0
c	c	u	b	c	u	0
u	u	u	u	u	u	0
0	0	0	0	0	0	0

Directoids: Ježek and Quackenbush

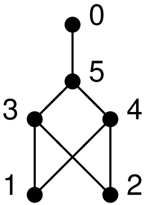
The directoid **D**:



$\cdot$	1	2	3	4	5	0
1	1	3	3	4	5	0
2	3	2	3	4	5	0
3	3	3	3	0	5	0
4	4	4	0	4	5	0
5	5	5	5	5	5	0
0	0	0	0	0	0	0

Directoids: Ježek and Quackenbush

The directoid **D**:

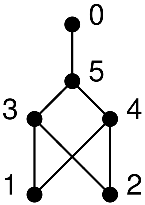


$\cdot$	1	2	3	4	5	0
1	1	3	3	4	5	0
2	3	2	3	4	5	0
3	3	3	3	0	5	0
4	4	4	0	4	5	0
5	5	5	5	5	5	0
0	0	0	0	0	0	0

The argument that **H** is INFB implies $\mathbf{D} \in \boldsymbol{V}(\mathbf{H})$.

Directoids: Ježek and Quackenbush

The directoid **D**:

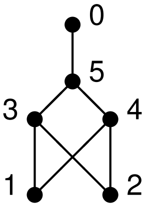


$\cdot$	1	2	3	4	5	0
1	1	3	3	4	5	0
2	3	2	3	4	5	0
3	3	3	3	0	5	0
4	4	4	0	4	5	0
5	5	5	5	5	5	0
0	0	0	0	0	0	0

The argument that **H** is INFB implies $\mathbf{D} \in \boldsymbol{V}(\mathbf{H})$.
But it's not.

Directoids: Ježek and Quackenbush

The directoid **D**:



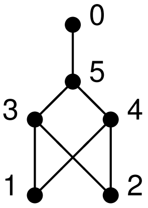
$\cdot$	1	2	3	4	5	0
1	1	3	3	4	5	0
2	3	2	3	4	5	0
3	3	3	3	0	5	0
4	4	4	0	4	5	0
5	5	5	5	5	5	0
0	0	0	0	0	0	0

The argument that **H** is INFB implies $\mathbf{D} \in \boldsymbol{V}(\mathbf{H})$.
But it's not. The calculator gives the equation

$$x_3((x_0x_1)(x_0(x_1x_2))) \approx (x_0x_1)(x_3(x_0(x_1x_2)))$$

Directoids: Ježek and Quackenbush

The directoid **D**:



$\cdot$	1	2	3	4	5	0
1	1	3	3	4	5	0
2	3	2	3	4	5	0
3	3	3	3	0	5	0
4	4	4	0	4	5	0
5	5	5	5	5	5	0
0	0	0	0	0	0	0

The argument that **H** is INFB implies $\mathbf{D} \in \boldsymbol{V}(\mathbf{H})$.
But it's not. The calculator gives the equation

$$x_3((x_0x_1)(x_0(x_1x_2))) \approx (x_0x_1)(x_3(x_0(x_1x_2)))$$

and claims it holds in **H** and fails in **D** under the substitution

$$x_0 \mapsto 1 \quad x_1 \mapsto 2 \quad x_2 \mapsto 4 \quad x_3 \mapsto 5$$

(Straightforward) Testing $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

(Straightforward) Testing $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

- Find a minimal sized generating set $\{g_0, \ldots, g_{k-1}\}$ of **B**.

(Straightforward) Testing $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

- Find a minimal sized generating set $\{g_0, \ldots, g_{k-1}\}$ of **B.**
- Start calculating $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(k) = \mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(x_0, \ldots, x_{k-1})$, keeping

(Straightforward) Testing $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

- Find a minimal sized generating set $\{g_0, \ldots, g_{k-1}\}$ of **B.**
- Start calculating $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(k) = \mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(x_0, \ldots, x_{k-1})$, keeping
  - A map from the elements to the term that gave them.

(Straightforward) Testing $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

- Find a minimal sized generating set $\{g_0, \ldots, g_{k-1}\}$ of $\mathbf{B}$.
- Start calculating $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(k) = \mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(x_0, \ldots, x_{k-1})$, keeping
  - A map from the elements to the term that gave them.
  - A partial homomorphism from $\varphi : \mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(k) \to \mathbf{B}$.

(Straightforward) Testing $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

- Find a minimal sized generating set $\{g_0, \ldots, g_{k-1}\}$ of $\mathbf{B}$.
- Start calculating $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(k) = \mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(x_0, \ldots, x_{k-1})$, keeping
  - A map from the elements to the term that gave them.
  - A partial homomorphism from $\varphi : \mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(k) \to \mathbf{B}$.
- If

  $$f(a_0, \ldots, a_{r-1}) = a$$

  is new, then

  $$\begin{aligned} t_a &= f(t_{a_0}, \ldots, t_{a_{r-1}}) \quad \text{and} \\ \varphi(a) &= f(\varphi(a_0), \ldots, \varphi(a_{r-1})) \end{aligned}$$

(Straightforward) Testing $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$

- Find a minimal sized generating set $\{g_0, \ldots, g_{k-1}\}$ of $\mathbf{B}$.
- Start calculating $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(k) = \mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(x_0, \ldots, x_{k-1})$, keeping
  - A map from the elements to the term that gave them.
  - A partial homomorphism from $\varphi : \mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(k) \to \mathbf{B}$.
- If $a = f(a_0, \ldots, a_{r-1})$ is **not** new, and

$$\varphi(a) \neq f(\varphi(a_0), \ldots, \varphi(a_{r-1}))$$

then the equation (of the Birkhoff basis):

$$t_a \approx f(t_{a_0}, \ldots, t_{a_{r-1}})$$

fails in $\mathbf{B}$ under the substitution $x_i \mapsto g_i$.

$\mathbf{D} \notin \boldsymbol{V}(\mathbf{H})$

- $x_3((x_0x_1)(x_0(x_1x_2))) \approx (x_0x_1)(x_3(x_0(x_1x_2)))$

  witnesses this (under 1 second).

$\mathbf{D} \notin \boldsymbol{V}(\mathbf{H})$

- $x_3((x_0x_1)(x_0(x_1x_2))) \approx (x_0x_1)(x_3(x_0(x_1x_2)))$
  witnesses this (under 1 second).
- $|\mathbf{F}_{\boldsymbol{V}(\mathbf{H})}(4)| = 26,467$ (60 minutes)

$\mathbf{D} \notin \boldsymbol{V}(\mathbf{H})$

- $x_3((x_0x_1)(x_0(x_1x_2))) \approx (x_0x_1)(x_3(x_0(x_1x_2)))$
  witnesses this (under 1 second).
- $|\mathbf{F}_{\boldsymbol{V}(\mathbf{H})}(4)| = 26,467$ (60 minutes)
- So the Birkhoff basis has over 700 million equations.

$\mathbf{D} \notin \boldsymbol{V}(\mathbf{H})$

- $x_3((x_0x_1)(x_0(x_1x_2))) \approx (x_0x_1)(x_3(x_0(x_1x_2)))$
  witnesses this (under 1 second).
- $|\mathbf{F}_{\boldsymbol{V}(\mathbf{H})}(4)| = 26,467$ (60 minutes)
- So the Birkhoff basis has over 700 million equations.
- Testing $\mathbf{H} \in \boldsymbol{V}(\mathbf{H})$ takes about 80 minutes.

$\mathrm{Cg}^{\mathbf{A}}(a, b)$ in Linear Time

Theorem

There is a linear time algorithm to compute $\mathrm{Cg}^{\mathbf{A}}(a, b)$ *for algebras* $\mathbf{A}$ *of a fixed similarity type having at least one, at least binary operation (and nearly linear even if it doesn't).*

Consequences

There are polynomial time algorithms for:

Consequences

There are polynomial time algorithms for:

- calculating the principal congruences of **A**

Consequences

There are polynomial time algorithms for:

- calculating the principal congruences of **A**
- calculating the join irreducible congruences of **A**

Consequences

There are polynomial time algorithms for:

- calculating the principal congruences of $\mathbf{A}$
- calculating the join irreducible congruences of $\mathbf{A}$
  - finding the TCT type set of $\mathbf{A}$

Consequences

There are polynomial time algorithms for:

- calculating the principal congruences of **A**
- calculating the join irreducible congruences of **A**
  - finding the TCT type set of **A**
- calculating the atoms of **Con** (**A**)

Consequences

There are polynomial time algorithms for:

- calculating the principal congruences of **A**
- calculating the join irreducible congruences of **A**
  - finding the TCT type set of **A**
- calculating the atoms of **Con** (**A**)
- deciding if **A** is simple; is subdirectly irreducible

Consequences

There are polynomial time algorithms for:

- calculating the principal congruences of $\mathbf{A}$
- calculating the join irreducible congruences of $\mathbf{A}$
  - finding the TCT type set of $\mathbf{A}$
- calculating the atoms of $\mathbf{Con}(\mathbf{A})$
- deciding if $\mathbf{A}$ is simple; is subdirectly irreducible
- (J. Demel) finding a subdirect decomposition of $\mathbf{A}$ into subdirectly irreducibles

Consequences

There are polynomial time algorithms for:

- calculating the principal congruences of **A**
- calculating the join irreducible congruences of **A**
  - finding the TCT type set of **A**
- calculating the atoms of **Con** (**A**)
- deciding if **A** is simple; is subdirectly irreducible
- (J. Demel) finding a subdirect decomposition of **A** into subdirectly irreducibles

But not for:

Consequences

There are polynomial time algorithms for:

- calculating the principal congruences of **A**
- calculating the join irreducible congruences of **A**
  - finding the TCT type set of **A**
- calculating the atoms of **Con** (**A**)
- deciding if **A** is simple; is subdirectly irreducible
- (J. Demel) finding a subdirect decomposition of **A** into subdirectly irreducibles

But not for:

- finding all of **Con** (**A**)

Consequences

There are polynomial time algorithms for:

- calculating the principal congruences of **A**
- calculating the join irreducible congruences of **A**
  - finding the TCT type set of **A**
- calculating the atoms of **Con** (**A**)
- deciding if **A** is simple; is subdirectly irreducible
- (J. Demel) finding a subdirect decomposition of **A** into subdirectly irreducibles

But not for:

- finding all of **Con** (**A**)
- finding all meet irreducibles of **Con** (**A**)

Consequences

There are polynomial time algorithms for:

- calculating the principal congruences of **A**
- calculating the join irreducible congruences of **A**
  - finding the TCT type set of **A**
- calculating the atoms of **Con** (**A**)
- deciding if **A** is simple; is subdirectly irreducible
- (J. Demel) finding a subdirect decomposition of **A** into subdirectly irreducibles

But not for:

- finding all of **Con** (**A**)
- finding all meet irreducibles of **Con** (**A**)
- finding all subdirect decompositions of **A**

Computing the TCT Type Set of **A**

Theorem (Berman, Kiss, Prőhle, Szendrei)

The TCT type of a cover $\alpha \prec \beta$ *in* **Con** $(\mathbf{A})$ *can be computed in time* $O(||\mathbf{A}||^4)$*.*

Computing the TCT Type Set of $\mathbf{A}$

Theorem (Berman, Kiss, Pröhle, Szendrei)

The TCT type of a cover $\alpha \prec \beta$ in $\mathbf{Con}\,(\mathbf{A})$ *can be computed in time* $O(||\mathbf{A}||^4)$.

Outline:

- We may assume $\beta \succ 0$.

Computing the TCT Type Set of $\mathbf{A}$

Theorem (Berman, Kiss, Prőhle, Szendrei)

The TCT type of a cover $\alpha \prec \beta$ in $\mathbf{Con}\,(\mathbf{A})$ *can be computed in time* $O(||\mathbf{A}||^4)$.

Outline:

- We may assume $\beta \succ 0$.
- Find a β subtrace (a two element subset, $\{a, b\}$, of a trace),

Computing the TCT Type Set of **A**

Theorem (Berman, Kiss, Prőhle, Szendrei)

The TCT type of a cover $\alpha \prec \beta$ in **Con** $(\mathbf{A})$ *can be computed in time* $O(||\mathbf{A}||^4)$.

Outline:

- We may assume $\beta \succ 0$.
- Find a β subtrace (a two element subset, $\{a, b\}$, of a trace), and deterimine if there is an involution (an $f \in \mathrm{Pol}_1(\mathbf{A})$ interchanging a and b) in time $O(||\mathbf{A}||^2)$.

Computing the TCT Type Set of $\mathbf{A}$

Theorem (Berman, Kiss, Prőhle, Szendrei)

The TCT type of a cover $\alpha \prec \beta$ in $\mathbf{Con}\,(\mathbf{A})$ *can be computed in time* $O(||\mathbf{A}||^4)$.

Outline:

- We may assume $\beta \succ 0$.
- Find a β subtrace (a two element subset, $\{a, b\}$, of a trace), and deterimine if there is an involution (an $f \in \mathrm{Pol}_1(\mathbf{A})$ interchanging a and b) in time $O(||\mathbf{A}||^2)$.
- Find the type of the subtrace.

Finding the type

Assume $\{a, b\}$ is a subtrace of $\beta \succ 0$. Let

$$\begin{aligned} \mathbf{T}_{a,b} &= \{(h(a,a), h(a,b), h(b,a), h(b,b)) : h \in \operatorname{Pol}_2 \mathbf{A}\} \\ &= \operatorname{Sg}_{\mathbf{A}^4}(\{(a,a,b,b), (a,b,a,b)\} \cup \Delta_4) \end{aligned}$$

Finding the type

Assume $\{a, b\}$ is a subtrace of $\beta \succ 0$. Let

$$\begin{aligned} \mathbf{T}_{a,b} &= \{(h(a,a), h(a,b), h(b,a), h(b,b)) : h \in \operatorname{Pol}_2 \mathbf{A}\} \\ &= \operatorname{Sg}_{\mathbf{A}^4}(\{(a,a,b,b),(a,b,a,b)\} \cup \Delta_4) \end{aligned}$$

We may think of the elements of $\mathbf{T}_{a,b}$ as 2×2 tables, like

	a	b
a	x	y
b	u	v

Finding the type

Assume $\{a, b\}$ is a subtrace of $\beta \succ 0$. Let

$$\begin{aligned}\mathbf{T}_{a,b} &= \{(h(a,a), h(a,b), h(b,a), h(b,b)) : h \in \mathrm{Pol}_2\, \mathbf{A}\} \\ &= \mathrm{Sg}_{\mathbf{A}^4}(\{(a,a,b,b), (a,b,a,b)\} \cup \Delta_4)\end{aligned}$$

We may think of the elements of $\mathbf{T}_{a,b}$ as 2×2 tables, like

$$\begin{array}{c|cc} & a & b \\ \hline a & x & y \\ b & u & v \end{array}$$

$$\begin{array}{c|cc} & a & b \\ \hline a & a & b \\ b & b & b \end{array} \qquad \begin{array}{c|cc} & a & b \\ \hline a & a & a \\ b & a & b \end{array}$$

are called a **join** and a **meet**.

Finding the type

While generating the universe of $\mathbf{T}_{a,b}$,

Finding the type

While generating the universe of $\mathbf{T}_{a,b}$,

- If a join or meet is found, record this. If $\{a, b\}$ has an involution, **stop**: the type is **3**.

Finding the type

While generating the universe of $\mathbf{T}_{a,b}$,

- If a join or meet is found, record this. If $\{a, b\}$ has an involution, **stop**: the type is **3**.
- If both a join and a meet are found, **stop**: the type is **4**.

Finding the type

While generating the universe of $\mathbf{T}_{a,b}$,

- If a join or meet is found, record this. If $\{a, b\}$ has an involution, **stop**: the type is **3**.
- If both a join and a meet are found, **stop**: the type is **4**.

In the other cases we must generate all of $\mathbf{T}_{a,b}$.

Finding the type

While generating the universe of $\mathbf{T}_{a,b}$,

- If a join or meet is found, record this. If $\{a, b\}$ has an involution, **stop**: the type is **3**.
- If both a join and a meet are found, **stop**: the type is **4**.

In the other cases we must generate all of $\mathbf{T}_{a,b}$.

- If a join or a meet was found, the type is **5**.

Finding the type

While generating the universe of $\mathbf{T}_{a,b}$,

- If a join or meet is found, record this. If $\{a, b\}$ has an involution, **stop**: the type is **3**.
- If both a join and a meet are found, **stop**: the type is **4**.

In the other cases we must generate all of $\mathbf{T}_{a,b}$.

- If a join or a meet was found, the type is **5**.
- If a **one-snag** was found, the type is **2**.

Finding the type

While generating the universe of $\mathbf{T}_{a,b}$,

- If a join or meet is found, record this. If $\{a, b\}$ has an involution, **stop**: the type is **3**.
- If both a join and a meet are found, **stop**: the type is **4**.

In the other cases we must generate all of $\mathbf{T}_{a,b}$.

- If a join or a meet was found, the type is **5**.
- If a **one-snag** was found, the type is **2**.
- Otherwise the type is **1**.

Computing the TCT Type Set of **A**

Theorem

The type of $\alpha \prec \beta$ *can be found in time* $O(||A||^3)$.

Computing the TCT Type Set of **A**

Theorem

The type of $\alpha \prec \beta$ can be found in time $O(||A||^3)$.

Theorem

Let $\mathbf{A}$ *be a finite algebra with n elements. Let $\beta \succ 0$ be an atom of* $\mathbf{Con}\,(\mathbf{A})$ *and let $\{a, b\}$ be two elements of a 0-β trace. The maximum size of $\mathbf{T}_{a,b}$ depending on the type of β over 0 is*

1 *or* **2**	n^3
5	$n^3/3 + n^2/2 + n/6$
4	$n^4/12 + n^3/3 + 5n^2/12 + n/6$
3	n^4

These bounds all obtain infinitely often.

Free Algebras: Birkhoff Construction of $\mathbf{F}_{V(\mathbf{A})}(X)$

Theorem (Birkhoff)

$\mathbf{F}_{V(\mathbf{A})}(X)$ is the subalgebra of $\mathbf{A}^{A^X}$ generated by $\{\bar{x} : x \in X\}$, where $\bar{x} \in \mathbf{A}^{A^X}$ is given by $\bar{x}_v = v(x)$ for $v \in A^X$.

Free Algebras: Birkhoff Construction of $\mathbf{F}_{V(\mathbf{A})}(X)$

Theorem (Birkhoff)

$\mathbf{F}_{V(\mathbf{A})}(X)$ is the subalgebra of $\mathbf{A}^{A^X}$ generated by $\{\bar{x} : x \in X\}$, where $\bar{x} \in \mathbf{A}^{A^X}$ is given by $\bar{x}_v = v(x)$ for $v \in A^X$.

- For $v \in A^X$ let $\mathbf{A}(v)$ be the subalgebra of $\mathbf{A}$ generated by $v(X)$.

Free Algebras: Birkhoff Construction of $\mathbf{F}_{V(\mathbf{A})}(X)$

Theorem (Birkhoff)

$\mathbf{F}_{V(\mathbf{A})}(X)$ is the subalgebra of $\mathbf{A}^{A^X}$ generated by $\{\bar{x} : x \in X\}$, where $\bar{x} \in \mathbf{A}^{A^X}$ is given by $\bar{x}_v = v(x)$ for $v \in A^X$.

- For $v \in A^X$ let $\mathbf{A}(v)$ be the subalgebra of $\mathbf{A}$ generated by $v(X)$.
- Let η_v be the kernel of $\mathbf{F}_{V(\mathbf{A})}(X) \to \mathbf{A}(v)$.

Free Algebras: Birkhoff Construction of $\mathbf{F}_{V(\mathbf{A})}(X)$

Theorem (Birkhoff)

$\mathbf{F}_{V(\mathbf{A})}(X)$ is the subalgebra of $\mathbf{A}^{A^X}$ generated by $\{\bar{x} : x \in X\}$, where $\bar{x} \in \mathbf{A}^{A^X}$ is given by $\bar{x}_v = v(x)$ for $v \in A^X$.

- For $v \in A^X$ let $\mathbf{A}(v)$ be the subalgebra of $\mathbf{A}$ generated by $v(X)$.
- Let η_v be the kernel of $\mathbf{F}_{V(\mathbf{A})}(X) \to \mathbf{A}(v)$.
- $\eta_v \leq \eta_u$ iff $v(x) \mapsto u(x)$, $x \in X$ extends to a homomorphism of $\mathbf{A}(v)$ onto $\mathbf{A}(u)$.

Free Algebras: Birkhoff Construction of $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(X)$

Theorem (Birkhoff)

$\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(X)$ is the subalgebra of $\mathbf{A}^{A^X}$ generated by $\{\bar{x} : x \in X\}$, where $\bar{x} \in \mathbf{A}^{A^X}$ is given by $\bar{x}_v = v(x)$ for $v \in A^X$.

- For $v \in A^X$ let $\mathbf{A}(v)$ be the subalgebra of $\mathbf{A}$ generated by $v(X)$.
- Let η_v be the kernel of $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(X) \to \mathbf{A}(v)$.
- $\eta_v \leq \eta_u$ iff $v(x) \mapsto u(x)$, $x \in X$ extends to a homomorphism of $\mathbf{A}(v)$ onto $\mathbf{A}(u)$.
- (Thinning) In this case the u coordinate can be eliminated.

Free Algebras: Birkhoff Construction of $\mathbf{F}_{V(\mathbf{A})}(X)$

Theorem (Birkhoff)

$\mathbf{F}_{V(\mathbf{A})}(X)$ is the subalgebra of $\mathbf{A}^{A^X}$ generated by $\{\bar{x} : x \in X\}$, where $\bar{x} \in \mathbf{A}^{A^X}$ is given by $\bar{x}_v = v(x)$ for $v \in A^X$.

- For $v \in A^X$ let $\mathbf{A}(v)$ be the subalgebra of $\mathbf{A}$ generated by $v(X)$.
- Let η_v be the kernel of $\mathbf{F}_{V(\mathbf{A})}(X) \to \mathbf{A}(v)$.
- $\eta_v \leq \eta_u$ iff $v(x) \mapsto u(x)$, $x \in X$ extends to a homomorphism of $\mathbf{A}(v)$ onto $\mathbf{A}(u)$.
- (Thinning) In this case the u coordinate can be eliminated.
- We can also eliminate u if $(v_1(x), v_2(x)) \mapsto u(x)$, $x \in X$ extends to a homomorphism of the subdirect product of $\mathbf{A}(v_1)$ and $\mathbf{A}(v_2)$ to $\mathbf{A}(u)$.

Free Algebras: Birkhoff Construction of $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(X)$

Theorem (Birkhoff)

$\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(X)$ is the subalgebra of $\mathbf{A}^{A^X}$ generated by $\{\bar{x} : x \in X\}$, where $\bar{x} \in \mathbf{A}^{A^X}$ is given by $\bar{x}_v = v(x)$ for $v \in A^X$.

- For $v \in A^X$ let $\mathbf{A}(v)$ be the subalgebra of $\mathbf{A}$ generated by $v(X)$.
- Let η_v be the kernel of $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(X) \to \mathbf{A}(v)$.
- $\eta_v \leq \eta_u$ iff $v(x) \mapsto u(x)$, $x \in X$ extends to a homomorphism of $\mathbf{A}(v)$ onto $\mathbf{A}(u)$.
- (Thinning) In this case the u coordinate can be eliminated.
- We can also eliminate u if $(v_1(x), v_2(x)) \mapsto u(x)$, $x \in X$ extends to a homomorphism of the subdirect product of $\mathbf{A}(v_1)$ and $\mathbf{A}(v_2)$ to $\mathbf{A}(u)$.
- But this takes too much time.

Free Algebras: Using Subdirect Decompositions

- Idea: find a subdirect decomposition of $\mathbf{A}(v)$ and replace $\mathbf{A}(v)$ with these si algebras. And then thin.

Free Algebras: Using Subdirect Decompositions

- Idea: find a subdirect decomposition of $\mathbf{A}(v)$ and replace $\mathbf{A}(v)$ with these si algebras. And then thin.
- While adding more coordinates, this allows for better thinning.

Free Algebras: Using Subdirect Decompositions

- Idea: find a subdirect decomposition of $\mathbf{A}(v)$ and replace $\mathbf{A}(v)$ with these si algebras. And then thin.
- While adding more coordinates, this allows for better thinning.
- Example: $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(4)$, for $\mathbf{A} = \mathbf{N}_5$.

Free Algebras: Using Subdirect Decompositions

- Idea: find a subdirect decomposition of $\mathbf{A}(v)$ and replace $\mathbf{A}(v)$ with these si algebras. And then thin.
- While adding more coordinates, this allows for better thinning.
- Example: $\mathbf{F}_{V(\mathbf{A})}(4)$, for $\mathbf{A} = \mathbf{N}_5$.
- Without thinning 625 coordinates.

Free Algebras: Using Subdirect Decompositions

- Idea: find a subdirect decomposition of $\mathbf{A}(v)$ and replace $\mathbf{A}(v)$ with these si algebras. And then thin.
- While adding more coordinates, this allows for better thinning.
- Example: $\mathbf{F}_{V(\mathbf{A})}(4)$, for $\mathbf{A} = \mathbf{N}_5$.
- Without thinning 625 coordinates.
- With thinning 132 coordinates: 24 copies of $\mathbf{4}$, 24 copies of $\mathbf{2} \times \mathbf{2}$, and 84 copies of $\mathbf{N}_5$.

Free Algebras: Using Subdirect Decompositions

- Idea: find a subdirect decomposition of $\mathbf{A}(v)$ and replace $\mathbf{A}(v)$ with these si algebras. And then thin.
- While adding more coordinates, this allows for better thinning.
- Example: $\mathbf{F}_{V(\mathbf{A})}(4)$, for $\mathbf{A} = \mathbf{N}_5$.
- Without thinning 625 coordinates.
- With thinning 132 coordinates: 24 copies of $\mathbf{4}$, 24 copies of $\mathbf{2} \times \mathbf{2}$, and 84 copies of $\mathbf{N}_5$.
- With decomposing and thinning only the 84 copies of $\mathbf{N}_5$.

Free Algebras: Using Subdirect Decompositions

- Idea: find a subdirect decomposition of $\mathbf{A}(v)$ and replace $\mathbf{A}(v)$ with these si algebras. And then thin.
- While adding more coordinates, this allows for better thinning.
- Example: $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(4)$, for $\mathbf{A} = \mathbf{N}_5$.
- Without thinning 625 coordinates.
- With thinning 132 coordinates: 24 copies of $\mathbf{4}$, 24 copies of $\mathbf{2} \times \mathbf{2}$, and 84 copies of $\mathbf{N}_5$.
- With decomposing and thinning only the 84 copies of $\mathbf{N}_5$.

In fact, every $\mathbf{F}_{\boldsymbol{V}(\mathbf{N}_5)}(k)$, $k \geq 3$, is a subdirect product of copies of $\mathbf{N}_5$.

Maltsev's Conditions

Jónsson's Terms

- A variety $\mathcal{V}$ is congruence distributive if and only if there are 3-ary terms $d_0, \ldots, d_k$ (called *Jónsson terms*) such that

$$
\begin{aligned}
d_0(x, y, z) &\approx x && \\
d_i(x, y, x) &\approx x && \text{for } 0 \leq i \leq k \\
d_i(x, x, y) &\approx d_{i+1}(x, x, y) && \text{for all even } i < k \\
d_i(x, y, y) &\approx d_{i+1}(x, y, y) && \text{for all odd } i < k \\
d_k(x, y, z) &\approx z.
\end{aligned}
\tag{1}
$$

Maltsev's Conditions

Jónsson's Terms

- A variety $\mathcal{V}$ is congruence distributive if and only if there are 3-ary terms $d_0, \ldots, d_k$ (called *Jónsson terms*) such that

$$\begin{aligned} d_0(x,y,z) &\approx x \\ d_i(x,y,x) &\approx x && \text{for } 0 \leq i \leq k \\ d_i(x,x,y) &\approx d_{i+1}(x,x,y) && \text{for all even } i < k \\ d_i(x,y,y) &\approx d_{i+1}(x,y,y) && \text{for all odd } i < k \\ d_k(x,y,z) &\approx z. \end{aligned} \tag{1}$$

  The *Jónsson level* of $\mathcal{V}$ is the least k.

Maltsev's Conditions

Jónsson's Terms

- A variety $\mathcal{V}$ is congruence distributive if and only if there are 3-ary terms $d_0, \dots, d_k$ (called *Jónsson terms*) such that

$$\begin{aligned} d_0(x,y,z) &\approx x \\ d_i(x,y,x) &\approx x && \text{for } 0 \leq i \leq k \\ d_i(x,x,y) &\approx d_{i+1}(x,x,y) && \text{for all even } i < k \\ d_i(x,y,y) &\approx d_{i+1}(x,y,y) && \text{for all odd } i < k \\ d_k(x,y,z) &\approx z. \end{aligned} \tag{1}$$

  The *Jónsson level* of $\mathcal{V}$ is the least k.
- How hard is it to test if $\boldsymbol{V}(\mathbf{A})$ is congruence distributive for a finite $\mathbf{A}$?

A Better Way

A Better Way

$(a, b, c)\ \rho\ (a', b', c')$ if $b = b'$ and either $a = a'$ **or** $c = c'$.

A Better Way

$(a, b, c) \ \rho \ (a', b', c')$ if $b = b'$ and either $a = a'$ **or** $c = c'$.

Theorem

Let $\mathcal{V}$ be a variety and let $\mathbf{S}$ *be the subalgebra of* $\mathbf{F}^3_{\mathcal{V}}(x, y)$ *generated by* (x, x, y), (x, y, x) *and* (y, x, x).

A Better Way

$(a, b, c)\ \rho\ (a', b', c')$ if $b = b'$ and either $a = a'$ **or** $c = c'$.

Theorem

Let $\mathcal{V}$ be a variety and let $\mathbf{S}$ *be the subalgebra of* $\mathbf{F}^3_{\mathcal{V}}(x, y)$ *generated by* (x, x, y)*,* (x, y, x) *and* (y, x, x)*.*

- *$\mathcal{V}$ is congruence distributive iff there is a ρ-path in S from (x, x, y) to (y, x, x), where the first link is ρ_{01}.*

A Better Way

$(a, b, c)\ \rho\ (a', b', c')$ if $b = b'$ and either $a = a'$ **or** $c = c'$.

Theorem

Let $\mathcal{V}$ be a variety and let $\mathbf{S}$ be the subalgebra of $\mathbf{F}^3_{\mathcal{V}}(x, y)$ generated by (x, x, y), (x, y, x) and (y, x, x).

- *$\mathcal{V}$ is congruence distributive iff there is a ρ-path in S from (x, x, y) to (y, x, x), where the first link is ρ_{01}.*
- *If $\mathcal{V}$ is congruence distributive then the Jónsson level of $\mathcal{V}$ is the length of the shortest such path.*

A Better Way

$(a, b, c)\ \rho\ (a', b', c')$ if $b = b'$ and either $a = a'$ **or** $c = c'$.

Theorem

Let $\mathcal{V}$ be a variety and let $\mathbf{S}$ be the subalgebra of $\mathbf{F}^3_{\mathcal{V}}(x, y)$ generated by (x, x, y), (x, y, x) and (y, x, x).

- *$\mathcal{V}$ is congruence distributive iff there is a ρ-path in S from (x, x, y) to (y, x, x), where the first link is ρ_{01}.*
- *If $\mathcal{V}$ is congruence distributive then the Jónsson level of $\mathcal{V}$ is the length of the shortest such path.*
- *Moreover, if $\mathcal{V}$ is congruence distributive then the Jónsson level is at most $2m - 2$, where $m = |\mathbf{F}_{\mathcal{V}}(x, y)|$ and this is the best possible bound in terms of m.*

A Better Way

Theorem

Let $\mathcal{V}$ be a variety and let $\mathbf{S}$ be the subalgebra of $\mathbf{F}^3_{\mathcal{V}}(x, y)$ generated by (x, x, y), (x, y, x) and (y, x, x).

- *$\mathcal{V}$ is congruence distributive iff there is a ρ-path in S from (x, x, y) to (y, x, x), where the first link is ρ_{01}.*
- *If $\mathcal{V}$ is congruence distributive then the Jónsson level of $\mathcal{V}$ is the length of the shortest such path.*
- *Moreover, if $\mathcal{V}$ is congruence distributive then the Jónsson level is at most $2m - 2$, where $m = |\mathbf{F}_{\mathcal{V}}(x, y)|$ and this is the best possible bound in terms of m.*

Proof.

More or less obvious,

A Better Way

Theorem

Let $\mathcal{V}$ be a variety and let $\mathbf{S}$ *be the subalgebra of* $\mathbf{F}^3_{\mathcal{V}}(x, y)$ *generated by* (x, x, y), (x, y, x) *and* (y, x, x).

- $\mathcal{V}$ *is congruence distributive iff there is a* ρ*-path in* S *from* (x, x, y) *to* (y, x, x)*, where the first link is* ρ_{01}.
- *If* $\mathcal{V}$ *is congruence distributive then the Jónsson level of* $\mathcal{V}$ *is the length of the shortest such path.*
- *Moreover, if* $\mathcal{V}$ *is congruence distributive then the Jónsson level is at most* $2m - 2$*, where* $m = |\mathbf{F}_{\mathcal{V}}(x, y)|$ *and this is the best possible bound in terms of* m.

Proof.

More or less obvious, (except the last part). □

Maltsev Conditions

Taylor Terms

Theorem (Siggers)

For a locally finite variety, having a Taylor term is a strong Maltsev condition.

Maltsev Conditions

Taylor Terms

Theorem (Siggers)

For a locally finite variety, having a Taylor term is a strong Maltsev condition.

- Variants of Siggers term have been given by several people.

Theorem (Siggers)

For a locally finite variety, having a Taylor term is a strong Maltsev condition.

- Variants of Siggers term have been given by several people.
- Matt Valeriote's talk will give some variants of Siggers original term that are best for our computational purposes, along with short proofs.

Maltsev Conditions

Congruence $SD_\wedge$

A **weak near unanimity term** is an idempotent term satisfying

$$t(y, x, \ldots, x) \approx t(x, y, \ldots, x) \approx \cdots \approx t(x, x, \ldots, y)$$

Theorem (Kozik)

A finitely generated variety is congruence $SD_\wedge$ iff it has wnu terms $w(x, y, z, u)$ and $s(x, y, z)$ satisfying

$$w(x, x, x, y) \approx s(x, x, y)$$

Maltsev Conditions

Theorem (Kozik)

A finitely generated variety is congruence $SD_\wedge$ iff it has wnu terms $w(x, y, z, u)$ and $s(x, y, z)$ satisfying

$$w(x, x, x, y) \approx s(x, x, y)$$

Corollary (M.Maroti and A. Janko)

A finitely generated variety is congruence $SD_\wedge$ iff it has a wnu term $s(x, y, z)$ and terms $r(x, y, z)$ and $t(x, y, z)$ satisfying

$$r(x, x, y) \approx r(x, y, x) \approx t(y, x, x) \approx t(x, y, x) \approx s(x, x, y)$$
$$r(y, x, x) \approx t(y, y, x)$$

Maltsev Conditions

Testing Congruence $SD_\wedge$

Form the subalgebra of $\mathbf{F}(x, y)^4$ generated by

$$(x, x, y, x) \quad (x, y, x, x) \quad (y, x, x, x)$$

Maltsev Conditions

Testing Congruence SD$_\wedge$

Form the subalgebra of $\mathbf{F}(x, y)^4$ generated by

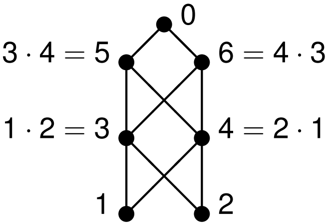
$$(x, x, y, x) \quad (x, y, x, x) \quad (y, x, x, x)$$

And look for elements of the form

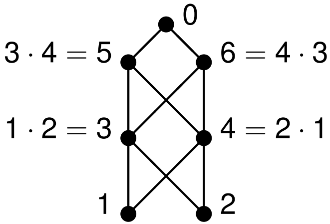
$$(a, a, a, x) \quad (a, a, b, x) \quad (b', a, a, x)$$

where $b' = \tau(b)$, where τ is the automorphism of $\mathbf{F}(x, y)$ interchanging x and y.

Directoids Again



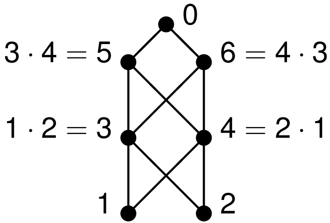
Directoids Again



The calculator found $\mathrm{SD}_\wedge$ terms:

$$
\begin{aligned}
r(x,y,z) &= yz \cdot (zy \cdot yx) \\
s(x,y,z) &= (xy \cdot yz)(zx \cdot xy) \\
t(x,y,z) &= (zx \cdot xy) \cdot yx
\end{aligned}
$$

Directoids Again



The calculator found $\mathrm{SD}_\wedge$ terms:

$$r(x,y,z) = yz \cdot (zy \cdot yx)$$
$$s(x,y,z) = (xy \cdot yz)(zx \cdot xy)$$
$$t(x,y,z) = (zx \cdot xy) \cdot yx$$

And also single wnu term $s(x,y,z)$ with $s(x,x,y) = s(y,y,x)$:

$$(xy \cdot yx)[(yz \cdot zx)(zy \cdot xz)]$$

Directoids Again

Theorem

The variety of directoids satisfies the Maltsev condition of the Corollary with

$$\begin{aligned} r(x,y,z) &= yz \cdot (zy \cdot yx) \\ s(x,y,z) &= (xy \cdot yz)(zx \cdot xy) \\ t(x,y,z) &= (zx \cdot xy) \cdot yx \end{aligned}$$

Directoids Again

Theorem

The variety of directoids satisfies the Maltsev condition of the Corollary with

$$r(x,y,z) = yz \cdot (zy \cdot yx)$$
$$s(x,y,z) = (xy \cdot yz)(zx \cdot xy)$$
$$t(x,y,z) = (zx \cdot xy) \cdot yx$$

The variety of directoids is congruence $SD_\wedge$ (using results of Kearnes, Kiss, and Szendrei).

Directoids Again

Theorem

The variety of directoids satisfies the Maltsev condition of the Corollary with

$$
\begin{aligned}
r(x,y,z) &= yz\cdot(zy\cdot yx)\\
s(x,y,z) &= (xy\cdot yz)(zx\cdot xy)\\
t(x,y,z) &= (zx\cdot xy)\cdot yx
\end{aligned}
$$

The variety of directoids is congruence $SD_\wedge$ (using results of Kearnes, Kiss, and Szendrei).

Proof.

$$r(x,x,y) = r(x,y,x) = t(y,x,x) = t(x,y,x) = s(x,x,y) = xy\cdot yx$$

$$r(y,x,x) = xy$$

$$t(x,x,y) = yx$$

$\square$

Directoids Again

Theorem

If $\mathcal{V}$ is a locally finite variety of directoids, it has a wnu term $s(x, y, z)$ satisfying

$$s(x, x, y) \approx s(y, y, x)$$

Directoids Again

Theorem

If $\mathcal{V}$ is a locally finite variety of directoids, it has a wnu term $s(x, y, z)$ satisfying

$$s(x, x, y) \approx s(y, y, x)$$

Proof.

- A finite directoid has a greatest element.

Directoids Again

Theorem

If $\mathcal{V}$ is a locally finite variety of directoids, it has a wnu term $s(x, y, z)$ satisfying

$$s(x, x, y) \approx s(y, y, x)$$

Proof.

- A finite directoid has a greatest element.
- If $s(x, y, z)$ is the top of $\mathbf{F}(x, y, z)$, then all maps of $\{x, y, z\}$ onto $\{x, y\}$ map s to the top of $\mathbf{F}(x, y)$.

Directoids Again

Theorem

If $\mathcal{V}$ is a locally finite variety of directoids, it has a wnu term $s(x, y, z)$ satisfying

$$s(x, x, y) \approx s(y, y, x)$$

Proof.

- A finite directoid has a greatest element.
- If $s(x, y, z)$ is the top of $\mathbf{F}(x, y, z)$, then all maps of $\{x, y, z\}$ onto $\{x, y\}$ map s to the top of $\mathbf{F}(x, y)$.
- So $s(x, y, z)$ is a wnu term and $s(x, x, y) = s(y, y, x)$.

$\square$

Directoids Again

Theorem

If $\mathcal{V}$ is a locally finite variety of directoids, it has a wnu term $s(x, y, z)$ satisfying

$$s(x, x, y) \approx s(y, y, x)$$

Proof.

- A finite directoid has a greatest element.
- If $s(x, y, z)$ is the top of $\mathbf{F}(x, y, z)$, then all maps of $\{x, y, z\}$ onto $\{x, y\}$ map s to the top of $\mathbf{F}(x, y)$.
- So $s(x, y, z)$ is a wnu term and $s(x, x, y) = s(y, y, x)$.

$\square$

Theorem

The variety of all directoids does not have such a term.

Directoids Again

Theorem

If $\mathcal{V}$ is a locally finite variety of directoids, it has a wnu term $s(x, y, z)$ satisfying

$$s(x, x, y) \approx s(y, y, x)$$

Proof.

- A finite directoid has a greatest element.
- If $s(x, y, z)$ is the top of $\mathbf{F}(x, y, z)$, then all maps of $\{x, y, z\}$ onto $\{x, y\}$ map s to the top of $\mathbf{F}(x, y)$.
- So $s(x, y, z)$ is a wnu term and $s(x, x, y) = s(y, y, x)$.

$\square$

Theorem

The variety of all directoids does not have such a term.

Proof.

Ježek and Quackenbush show directoids do not have a term satisfying $u(x, y) \approx u(y, x)$. $\square$

Testing Primality

Theorem (Clark, Davey, Pitkethly, Rifqui; McKenzie)

Let **A** *be an algebra on* $\{0, 1, \ldots, n-1\}$*.* **A** *is primal iff*

Testing Primality

Theorem (Clark, Davey, Pitkethly, Rifqui; McKenzie)

Let $\mathbf{A}$ *be an algebra on* $\{0, 1, \ldots, n-1\}$*.* $\mathbf{A}$ *is primal iff*

- *the subalgebra of* $\mathbf{A}^4$ *generated by* $(0, 0, 1, 1)$ *and* $(0, 1, 0, 1)$ *contains* $(0, 0, 0, 1)$ *(the meet), and*

Testing Primality

Theorem (Clark, Davey, Pitkethly, Rifqui; McKenzie)

Let $\mathbf{A}$ *be an algebra on* $\{0, 1, \ldots, n-1\}$. $\mathbf{A}$ *is primal iff*

- *the subalgebra of* $\mathbf{A}^4$ *generated by* $(0,0,1,1)$ *and* $(0,1,0,1)$ *contains* $(0,0,0,1)$ *(the meet), and*
- $\mathbf{F}_{V(\mathbf{A})}(1) \leq \mathbf{A}^n$ *contains*

$$\chi_0 = (1, 0, \ldots, 0),$$
$$\vdots$$
$$\chi_{n-1} = (0, \ldots, 0, 1),$$

and

Testing Primality

Theorem (Clark, Davey, Pitkethly, Rifqui; McKenzie)

Let $\mathbf{A}$ *be an algebra on* $\{0, 1, \ldots, n-1\}$*.* $\mathbf{A}$ *is primal iff*

- *the subalgebra of* $\mathbf{A}^4$ *generated by* $(0, 0, 1, 1)$ *and* $(0, 1, 0, 1)$ *contains* $(0, 0, 0, 1)$ *(the meet), and*
- $\mathbf{F}_{V(\mathbf{A})}(1) \leq \mathbf{A}^n$ *contains*

$$\begin{aligned} \chi_0 &= (1, 0, \ldots, 0), \\ &\vdots \\ \chi_{n-1} &= (0, \ldots, 0, 1), \end{aligned}$$

  and
- *the subalgebra of* $\mathbf{F}_{V(\mathbf{A})}(1)$ *generated by the* χ_i*'s includes* $(0, 1, \ldots, n-1)$*.*

Day Quadruples

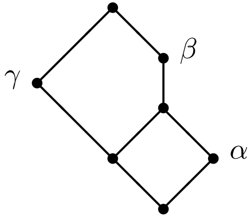
Let a, b, c and $d \in \mathbf{A}$ and let

$$\alpha = \mathrm{Cg}^{\mathbf{A}}(c, d) \quad \beta = \mathrm{Cg}^{\mathbf{A}}((a, b)(c, d)) \quad \gamma = \mathrm{Cg}^{\mathbf{A}}((a, c)(b, d))$$

Day Quadruples

Let a, b, c and $d \in \mathbf{A}$ and let

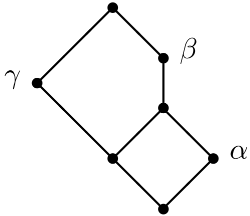
$$\alpha = \mathrm{Cg}^{\mathbf{A}}(c, d) \quad \beta = \mathrm{Cg}^{\mathbf{A}}((a, b)(c, d)) \quad \gamma = \mathrm{Cg}^{\mathbf{A}}((a, c)(b, d))$$



Day Quadruples

Let a, b, c and $d \in \mathbf{A}$ and let

$$\alpha = \mathrm{Cg}^{\mathbf{A}}(c,d) \quad \beta = \mathrm{Cg}^{\mathbf{A}}((a,b)(c,d)) \quad \gamma = \mathrm{Cg}^{\mathbf{A}}((a,c)(b,d))$$



(a,b,c,d) is a **Day quadruple** if in the subalgebra $\mathbf{B}$ generated by $\{a,b,c,d\}$

$$(a,b) \notin \mathrm{Cg}^{\mathbf{B}}(c,d) \vee [\mathrm{Cg}^{\mathbf{B}}((a,b)(c,d)) \wedge \mathrm{Cg}^{\mathbf{B}}((a,c)(b,d))]$$

Polynomial Algorithms for Idempotent Algebras

Theorem (Freese, Valeriote)

Let $\mathbf{A}$ *be a finite idempotent algebra and* $\mathcal{V}$ *be the variety it generates. Then* $\mathcal{V}$ *fails to be congruence modular if and only if there is a Day quadruple,* (a, b, c, d) *in* $\mathbf{A}^2$*.*

Polynomial Algorithms for Idempotent Algebras

Theorem (Freese, Valeriote)

Let $\mathbf{A}$ *be a finite idempotent algebra and* $\mathcal{V}$ *be the variety it generates. Then* $\mathcal{V}$ *fails to be congruence modular if and only if there is a Day quadruple,* (a, b, c, d) *in* $\mathbf{A}^2$*.*

Moreover, this Day quadruple can be chosen so that

- *there exist* x_0*,* x_1*,* y_0*,* y_1 *in* $\mathbf{A}$ *such that* $a = (x_0, x_1)$*,* $b = (x_0, y_1)$*,* $c = (y_0, x_1)$*, and* $d = (y_0, y_1)$*;*

Polynomial Algorithms for Idempotent Algebras

$$n = |\mathbf{A}|$$

$$m = ||\mathbf{A}|| = \sum_{i=0}^{r} k_i n^i$$

$$r = \text{the largest arity of the operations of } \mathbf{A}$$

$$(k_i = \text{the number of basic operations of arity } i)$$

Polynomial Algorithms for Idempotent Algebras

Theorem (Freese, Valeriote)

Let $\mathbf{A}$ *be a finite idempotent algebra with parameters as above. Then each of the following can be determined in the time indicated:*

$\boldsymbol{V}(\mathbf{A})$ *is congruence modular:* crn^4m^2.

Polynomial Algorithms for Idempotent Algebras

Theorem (Freese, Valeriote)

Let $\mathbf{A}$ *be a finite idempotent algebra with parameters as above. Then each of the following can be determined in the time indicated:*

$\boldsymbol{V}(\mathbf{A})$ *is congruence modular:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence distributive:*	$crn^4 m^2$.

Polynomial Algorithms for Idempotent Algebras

Theorem (Freese, Valeriote)

Let $\mathbf{A}$ *be a finite idempotent algebra with parameters as above. Then each of the following can be determined in the time indicated:*

$\boldsymbol{V}(\mathbf{A})$ *is congruence modular:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence distributive:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence semidistributive:*	$crn^2 m^2$.

Polynomial Algorithms for Idempotent Algebras

Theorem (Freese, Valeriote)

Let **A** *be a finite idempotent algebra with parameters as above. Then each of the following can be determined in the time indicated:*

$\boldsymbol{V}(\mathbf{A})$ *is congruence modular:*	crn^4m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence distributive:*	crn^4m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence semidistributive:*	crn^2m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence meet semidistributive:*	crn^2m^2.

Polynomial Algorithms for Idempotent Algebras

Theorem (Freese, Valeriote)

Let $\mathbf{A}$ *be a finite idempotent algebra with parameters as above. Then each of the following can be determined in the time indicated:*

$\boldsymbol{V}(\mathbf{A})$ *is congruence modular:*	crn^4m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence distributive:*	crn^4m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence semidistributive:*	crn^2m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence meet semidistributive:*	crn^2m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence permutable:*	crn^4m^2.

Polynomial Algorithms for Idempotent Algebras

Theorem (Freese, Valeriote)

Let $\mathbf{A}$ *be a finite idempotent algebra with parameters as above. Then each of the following can be determined in the time indicated:*

$\boldsymbol{V}(\mathbf{A})$ *is congruence modular:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence distributive:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence semidistributive:*	$crn^2 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence meet semidistributive:*	$crn^2 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence permutable:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence* k*-permutable for some* k*:*	$crn^3 m$.

Polynomial Algorithms for Idempotent Algebras

Theorem (Freese, Valeriote)

Let **A** *be a finite idempotent algebra with parameters as above. Then each of the following can be determined in the time indicated:*

$\boldsymbol{V}(\mathbf{A})$ *is congruence modular:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence distributive:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence semidistributive:*	$crn^2 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence meet semidistributive:*	$crn^2 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence permutable:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence k-permutable for some k:*	$crn^3 m$.
A *has a Taylor term:*	$crn^3 m$.

Polynomial Algorithms for Idempotent Algebras

Theorem (Freese, Valeriote)

Let **A** *be a finite idempotent algebra with parameters as above. Then each of the following can be determined in the time indicated:*

$\boldsymbol{V}(\mathbf{A})$ *is congruence modular:*	crn^4m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence distributive:*	crn^4m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence semidistributive:*	crn^2m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence meet semidistributive:*	crn^2m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence permutable:*	crn^4m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence k-permutable for some k:*	crn^3m.
A *has a Taylor term:*	crn^3m.
A *has a Hobby-McKenzie term:*	crn^3m.

Polynomial Algorithms for Idempotent Algebras

Theorem (Freese, Valeriote)

Let $\mathbf{A}$ *be a finite idempotent algebra with parameters as above. Then each of the following can be determined in the time indicated:*

$\boldsymbol{V}(\mathbf{A})$ *is congruence modular:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence distributive:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence semidistributive:*	$crn^2 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence meet semidistributive:*	$crn^2 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence permutable:*	$crn^4 m^2$.
$\boldsymbol{V}(\mathbf{A})$ *is congruence* k*-permutable for some* k*:*	$crn^3 m$.
$\mathbf{A}$ *has a Taylor term:*	$crn^3 m$.
$\mathbf{A}$ *has a Hobby-McKenzie term:*	$crn^3 m$.
$\mathbf{A}$ *has a majority term:*	$crn^6 m^2$.

Polynomial Algorithms for Idempotent Algebras

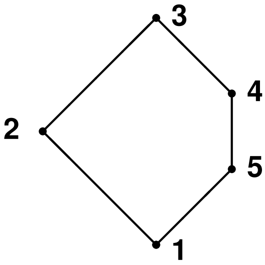
Theorem (Freese, Valeriote)

Let **A** *be a finite idempotent algebra with parameters as above. Then each of the following can be determined in the time indicated:*

	$\boldsymbol{V}(\mathbf{A})$ *is congruence modular:*	crn^4m^2.
	$\boldsymbol{V}(\mathbf{A})$ *is congruence distributive:*	crn^4m^2.
->	$\boldsymbol{V}(\mathbf{A})$ *is congruence semidistributive:*	crn^2m^2.
->	$\boldsymbol{V}(\mathbf{A})$ *is congruence meet semidistributive:*	crn^2m^2.
	$\boldsymbol{V}(\mathbf{A})$ *is congruence permutable:*	crn^4m^2.
->	$\boldsymbol{V}(\mathbf{A})$ *is congruence k-permutable for some k:*	crn^3m.
->	**A** *has a Taylor term:*	crn^3m.
->	**A** *has a Hobby-McKenzie term:*	crn^3m.
	A *has a majority term:*	crn^6m^2.

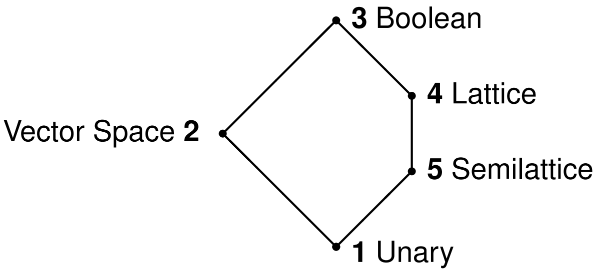
Polynomial Algorithms for Idempotent Algebras

TCT Types



Polynomial Algorithms for Idempotent Algebras

TCT Types



Theorem (Szendrei, Valeriote)

- *Let T be a proper order ideal of the lattice of types, and*
- *let $\mathbf{A}$ be a finite idempotent algebra that fails to omit T.*

Theorem (Szendrei, Valeriote)

- *Let T be a proper order ideal of the lattice of types, and*
- *let $\mathbf{A}$ be a finite idempotent algebra that fails to omit T.*

Then a witness of this failure can be found in a strictly simple algebra $\mathbf{S}$ in $\boldsymbol{HS}(\mathbf{A})$.

Theorem (Szendrei, Valeriote)

- *Let T be a proper order ideal of the lattice of types, and*
- *let **A** be a finite idempotent algebra that fails to omit T.*

*Then a witness of this failure can be found in a strictly simple algebra **S** in **HS**(**A**).*

*If **S** is a strictly simple idempotent algebra of TCT type **1**, **4**, or **5**, then* $|\mathbf{S}| = 2$.

Theorem (Szendrei, Valeriote)

- *Let T be a proper order ideal of the lattice of types, and*
- *let* $\mathbf{A}$ *be a finite idempotent algebra that fails to omit T.*

Then a witness of this failure can be found in a strictly simple algebra $\mathbf{S}$ *in* $\boldsymbol{HS}(\mathbf{A})$.

If $\mathbf{S}$ *is a strictly simple idempotent algebra of TCT type* $\mathbf{1}$, $\mathbf{4}$, *or* $\mathbf{5}$, *then* $|\mathbf{S}| = 2$.

Theorem

Let $\mathbf{A}$ *be finite indempotent, and let* $\mathbf{S} \in \boldsymbol{HS}(\mathbf{A})$ *be strictly simple. Then*

- *there are $a, b \in A$ such that, if* $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}(a, b)$, *then*
- $\mathrm{Cg}^{\mathbf{B}}(a, b) = 1_B$ *and is join irreducible with lower cover ρ such that* $\mathbf{B}/\rho = \mathbf{S}$.

The End

The End

UACalc Web Site:

http://uacalc.org/