Cyclic terms for join semi-distributive varieties I

Libor Barto

joint work with Marcin Kozik

Department of Algebra
Faculty of Mathematics and Physics
Charles University in Prague
Czech Republic

AAA Bern 2009

WNUs

Definition

w is a weak near-unanimity operation (WNU), if

- *w is idempotent* $\quad w(x, x, \ldots, x) = x$
- $w(x, x, \ldots, x, y) = w(x, x, \ldots, x, y, x) = \cdots = w(y, x, x, \ldots, x)$.

WNUs

Definition

w is a weak near-unanimity operation (WNU), if

- *w is idempotent* $w(x, x, \dots, x) = x$
- $w(x, x, \dots, x, y) = w(x, x, \dots, x, y, x) = \dots = w(y, x, x, \dots, x)$.

Theorem (TCT (Hobby, McKenzie), Taylor)

For a locally finite variety $\mathcal{V}$ TFAE

- *$\mathcal{V}$ omits type 1*
- *$\mathcal{V}$ satisfies some nontrivial idempotent Maltsev condition*
- *$\mathcal{V}$ has a Taylor term*

WNUs

Definition

w is a weak near-unanimity operation (WNU), if

- *w is idempotent* $\quad w(x, x, \ldots, x) = x$
- $w(x, x, \ldots, x, y) = w(x, x, \ldots, x, y, x) = \cdots = w(y, x, x, \ldots, x)$.

Theorem (TCT (Hobby, McKenzie), Taylor)

For a locally finite variety $\mathcal{V}$ TFAE

- *$\mathcal{V}$ omits type 1*
- *$\mathcal{V}$ satisfies some nontrivial idempotent Maltsev condition*
- *$\mathcal{V}$ has a Taylor term*

Theorem (Maróti, McKenzie 06)

- *$\mathcal{V}$ has a WNU term*

Cyclic operation

Definition

t is a cyclic operation, if

- *t is idempotent* $\quad t(x, x, \ldots, x) = x$
- $t(x_1, x_2, \ldots, x_n) = t(x_2, x_3, \ldots, x_n, x_1)$.

Cyclic operation

Definition

t is a cyclic operation, if

- *t is idempotent* $\quad t(x, x, \ldots, x) = x$
- $t(x_1, x_2, \ldots, x_n) = t(x_2, x_3, \ldots, x_n, x_1)$.

Every cyclic operation is a WNU

Cyclic operation

Definition

t is a cyclic operation, if

- *t is idempotent* $\quad t(x, x, \ldots, x) = x$
- $t(x_1, x_2, \ldots, x_n) = t(x_2, x_3, \ldots, x_n, x_1)$.

Every cyclic operation is a WNU

Motivation for cyclic and WNU operations: The complexity of Constraint Satisfaction Problems

The (hi)story of cyclic terms

Theorems

Let $\mathcal{V} = HSP(\mathbf{A})$, $\mathbf{A}$ *finite. If*

Then $\mathbf{A}$ *(thus* $\mathcal{V}$*) has a* p*-ary cyclic term for all primes* $p > |A|$.

The (hi)story of cyclic terms

Theorems

Let $\mathcal{V} = HSP(\mathbf{A})$, $\mathbf{A}$ finite. If

- $|A| \leq 3$ *and* $\mathcal{V}$ *has a majority term (07 Kozik, Marković, Stanovský & Computer)*

Then $\mathbf{A}$ *(thus* $\mathcal{V}$*) has a* p*-ary cyclic term for all primes* $p > |A|$*.*

The (hi)story of cyclic terms

Theorems

Let $\mathcal{V} = HSP(\mathbf{A})$, $\mathbf{A}$ finite. If

- $|A| \leq 3$ *and* $\mathcal{V}$ *has a majority term (07 Kozik, Marković, Stanovský & Computer)*
- $\mathcal{V}$ *has a majority term (07 Barto, Kozik, Niven)*

Then $\mathbf{A}$ *(thus* $\mathcal{V}$*) has a p-ary cyclic term for all primes* $p > |A|$.

The (hi)story of cyclic terms

Theorems

Let $\mathcal{V} = HSP(\mathbf{A})$, $\mathbf{A}$ finite. If

- $|A| \leq 3$ *and* $\mathcal{V}$ *has a majority term (07 Kozik, Marković, Stanovský & Computer)*
- $\mathcal{V}$ *has a majority term (07 Barto, Kozik, Niven)*
- $\mathcal{V}$ *is congruence distributive (07 BKN)*

Then $\mathbf{A}$ *(thus* $\mathcal{V}$*) has a p-ary cyclic term for all primes* $p > |A|$.

The (hi)story of cyclic terms

Theorems

Let $\mathcal{V} = HSP(\mathbf{A})$, $\mathbf{A}$ finite. If

- $|A| \leq 3$ *and* $\mathcal{V}$ *has a majority term (07 Kozik, Marković, Stanovský & Computer)*
- $\mathcal{V}$ *has a majority term (07 Barto, Kozik, Niven)*
- $\mathcal{V}$ *is congruence distributive (07 BKN)*
- $\mathcal{V}$ *is congruence modular (07 Maróti, McKenzie)*

Then $\mathbf{A}$ *(thus* $\mathcal{V}$*) has a p-ary cyclic term for all primes* $p > |A|$.

The (hi)story of cyclic terms

Theorems

Let $\mathcal{V} = HSP(\mathbf{A})$, $\mathbf{A}$ *finite. If*

- $|A| \leq 3$ *and* $\mathcal{V}$ *has a majority term (07 Kozik, Marković, Stanovský & Computer)*
- $\mathcal{V}$ *has a majority term (07 Barto, Kozik, Niven)*
- $\mathcal{V}$ *is congruence distributive (07 BKN)*
- $\mathcal{V}$ *is congruence modular (07 Maróti, McKenzie)*
- $\mathcal{V}$ *is congruence join semi-distributive (07 BKN)*

Then $\mathbf{A}$ *(thus* $\mathcal{V}$*) has a p-ary cyclic term for all primes* $p > |A|$.

The (hi)story of cyclic terms

Theorems

Let $\mathcal{V} = HSP(\mathbf{A})$, $\mathbf{A}$ finite. If

- $|A| \leq 3$ *and* $\mathcal{V}$ *has a majority term (07 Kozik, Marković, Stanovský & Computer)*
- $\mathcal{V}$ *has a majority term (07 Barto, Kozik, Niven)*
- $\mathcal{V}$ *is congruence distributive (07 BKN)*
- $\mathcal{V}$ *is congruence modular (07 Maróti, McKenzie)*
- $\mathcal{V}$ *is congruence join semi-distributive (07 BKN)*
- $\mathcal{V}$ *is congruence join semi-distributive (08 BK)*

Then $\mathbf{A}$ *(thus* $\mathcal{V}$*) has a p-ary cyclic term for all primes* $p > |A|$.

The (hi)story of cyclic terms

Theorems

Let $\mathcal{V} = HSP(\mathbf{A})$, $\mathbf{A}$ finite. If

- $|A| \leq 3$ *and* $\mathcal{V}$ *has a majority term (07 Kozik, Marković, Stanovský & Computer)*
- $\mathcal{V}$ *has a majority term (07 Barto, Kozik, Niven)*
- $\mathcal{V}$ *is congruence distributive (07 BKN)*
- $\mathcal{V}$ *is congruence modular (07 Maróti, McKenzie)*
- $\mathcal{V}$ *is congruence join semi-distributive (07 BKN)*
- $\mathcal{V}$ *is congruence join semi-distributive (08 BK)*
- $\mathcal{V}$ *omits* 1 *(09 BK)*

Then $\mathbf{A}$ *(thus* $\mathcal{V}$*) has a p-ary cyclic term for all primes* $p > |A|$.

Remarks

- Finite generation is necessary: There exists a locally finite variety omitting 1 with no cyclic terms.

Remarks

- Finite generation is necessary: There exists a locally finite variety omitting 1 with no cyclic terms.
- It easily follows that **A** has an n-ary cyclic term for every n which is a product of primes $> |A|$.

Remarks

- Finite generation is necessary: There exists a locally finite variety omitting 1 with no cyclic terms.
- It easily follows that **A** has an n-ary cyclic term for every n which is a product of primes $> |A|$.
- We can't want more: There exists a finitely generated variety omitting 1 with no cyclic term of any other arity.

Remarks

- Finite generation is necessary: There exists a locally finite variety omitting 1 with no cyclic terms.
- It easily follows that **A** has an n-ary cyclic term for every n which is a product of primes $> |A|$.
- We can't want more: There exists a finitely generated variety omitting 1 with no cyclic term of any other arity.
- It follows that a localy finite variety has a p-ary WNU for every prime greater than the size of the two-generated free algebra.

$SD(\vee)$

Definition

A lattice L is join semi-distributive, if

$$\forall a, b, c \in L \qquad a \vee b = a \vee c \;\Rightarrow\; a \vee b = a \vee (b \wedge c)$$

$SD(\vee)$

Definition

A lattice L is join semi-distributive, if

$$\forall a, b, c \in L \qquad a \vee b = a \vee c \;\Rightarrow\; a \vee b = a \vee (b \wedge c)$$

A variety $\mathcal{V}$ is congruence join semi-distributive ($SD(\vee)$), if all algebras in $\mathcal{V}$ has join semi-distributive congruence lattices

$SD(\vee)$

Definition

A lattice L is join semi-distributive, if

$$\forall a, b, c \in L \qquad a \vee b = a \vee c \;\Rightarrow\; a \vee b = a \vee (b \wedge c)$$

A variety $\mathcal{V}$ is congruence join semi-distributive ($SD(\vee)$), if all algebras in $\mathcal{V}$ has join semi-distributive congruence lattices

Theorem (TCT + Kearnes 01)

For a locally finite variety $\mathcal{V}$ TFAE

- $\mathcal{V}$ *is* $SD(\vee)$
- $\mathcal{V}$ *omits* $1, 2$ *and* 5
- $\mathcal{V}$ *satisfies certain Maltsev condition involving linear equations only*

Cyclic subpowers

Definition

Let $\mathbf{A}$ be a finite algebra. A subalgebra $\mathbf{R} \leq \mathbf{A}^n$ is called cyclic, if

$$\forall a_1, \dots, a_n \in A \qquad (a_1, a_2, \dots, a_n) \in R \Rightarrow (a_2, \dots, a_n, a_1) \in R$$

Cyclic subpowers

Definition

Let $\mathbf{A}$ *be a finite algebra. A subalgebra* $\mathbf{R} \leq \mathbf{A}^n$ *is called cyclic, if*

$$\forall a_1, \dots, a_n \in A \qquad (a_1, a_2, \dots, a_n) \in R \Rightarrow (a_2, \dots, a_n, a_1) \in R$$

Lemma

If all nonempty cyclic subalgebras of $\mathbf{A}^p$ *contain a constant tuple, then* $\mathbf{A}$ *has a p-ary cyclic term.*

Lemma

If all nonempty cyclic subalgebras of $\mathbf{A}^p$ contain a constant tuple, then $\mathbf{A}$ has a p-ary cyclic term.

Proof.

$\square$

Why cyclic subpowers?

Lemma

If all nonempty cyclic subalgebras of $\mathbf{A}^p$ contain a constant tuple, then $\mathbf{A}$ has a p-ary cyclic term.

Proof.

- For every tuple $\mathbf{a} = (a_1, \dots, a_p)$, consider $R_{\mathbf{a}} = Sg((a_1, \dots, a_p), (a_2, \dots, a_p, a_1), \dots) \leq \mathbf{A}^p$

$\square$

Why cyclic subpowers?

Lemma

If all nonempty cyclic subalgebras of $\mathbf{A}^p$ contain a constant tuple, then $\mathbf{A}$ has a p-ary cyclic term.

Proof.

- For every tuple $\mathbf{a} = (a_1, \dots, a_p)$, consider $R_{\mathbf{a}} = Sg((a_1, \dots, a_p), (a_2, \dots, a_p, a_1), \dots) \leq \mathbf{A}^p$
- $R_{\mathbf{a}}$ contains a constant tuple $\Rightarrow$ there exists a term $t_{\mathbf{a}}$ such that

$$t_{\mathbf{a}}(a_1, a_2, \dots, a_p) = t_{\mathbf{a}}(a_2, \dots, a_p, a_1) = \dots$$

□

Why cyclic subpowers?

Lemma

If all nonempty cyclic subalgebras of $\mathbf{A}^p$ contain a constant tuple, then $\mathbf{A}$ has a p-ary cyclic term.

Proof.

- For every tuple $\mathbf{a} = (a_1, \dots, a_p)$, consider $R_{\mathbf{a}} = Sg((a_1, \dots, a_p), (a_2, \dots, a_p, a_1), \dots) \leq \mathbf{A}^p$
- $R_{\mathbf{a}}$ contains a constant tuple $\Rightarrow$ there exists a term $t_{\mathbf{a}}$ such that

$$t_{\mathbf{a}}(a_1, a_2, \dots, a_p) = t_{\mathbf{a}}(a_2, \dots, a_p, a_1) = \dots$$

- By composing these terms (in certain way) we get a cyclic term

□

Properties of a minimal counterexample

Fix a prime p. We consider a minimal counterexample to the assumption of the last lemma (and we want to get a contradiction):

Properties of a minimal counterexample

Fix a prime p. We consider a minimal counterexample to the assumption of the last lemma (and we want to get a contradiction):

Let $\mathbf{A}$ be a minimal $SD(\vee)$ algebra ($|A| < p$) st. there exists a nonempty cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant tuple

Properties of a minimal counterexample

Fix a prime p. We consider a minimal counterexample to the assumption of the last lemma (and we want to get a contradiction):

Let $\mathbf{A}$ be a minimal $SD(\vee)$ algebra ($|A| < p$) st. there exists a nonempty cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant tuple

- $\mathbf{R}$ is subdirect

Properties of a minimal counterexample

Fix a prime p. We consider a minimal counterexample to the assumption of the last lemma (and we want to get a contradiction):

Let $\mathbf{A}$ be a minimal $SD(\vee)$ algebra ($|A| < p$) st. there exists a nonempty cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant tuple

- $\mathbf{R}$ is subdirect
- $\mathbf{A}$ is simple

Properties of a minimal counterexample

Fix a prime p. We consider a minimal counterexample to the assumption of the last lemma (and we want to get a contradiction):

Let $\mathbf{A}$ be a minimal $SD(\vee)$ algebra ($|A| < p$) st. there exists a nonempty cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant tuple

- $\mathbf{R}$ is subdirect
- $\mathbf{A}$ is simple
- The core theorem (Marcin's talk): There exists a nonidentical retraction $f : (A, R) \to (A, R)$,

Properties of a minimal counterexample

Fix a prime p. We consider a minimal counterexample to the assumption of the last lemma (and we want to get a contradiction):

Let $\mathbf{A}$ be a minimal $SD(\vee)$ algebra ($|A| < p$) st. there exists a nonempty cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant tuple

- $\mathbf{R}$ is subdirect
- $\mathbf{A}$ is simple
- The core theorem (Marcin's talk): There exists a nonidentical retraction $f : (A, R) \to (A, R)$,

  i.e. a mapping $f : A \to A$, $f \neq id$ s.t.
  - $f^2 = f$ (i.e. f is identical on its image)
  - if $(a_1, \ldots, a_p) \in R$, then $(f(a_1), \ldots, f(a_p)) \in R$

Q.E.D.

$\mathbf{A}$: minimal $SD(\vee)$ algebra st. $\exists$ cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant

- The core theorem (Marcin's talk): There exists a nonidentical retraction $f : (A, R) \to (A, R)$, i.e. a mapping $f : A \to A$, $f \neq id$ s.t.
  - $f^2 = f$ (i.e. f is identical on its image)
  - if $(a_1, \dots, a_p) \in R$, then $(f(a_1), \dots, f(a_p)) \in R$

Q.E.D.

A: minimal $SD(\vee)$ algebra st. $\exists$ cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant

- The core theorem (Marcin's talk): There exists a nonidentical retraction $f : (A, R) \to (A, R)$, i.e. a mapping $f : A \to A$, $f \neq id$ s.t.
  - $f^2 = f$ (i.e. f is identical on its image)
  - if $(a_1, \dots, a_p) \in R$, then $(f(a_1), \dots, f(a_p)) \in R$
- Assume $\mathbf{A} = (A, t_1, \dots, t_m)$, where $t_1, \dots, t_m$ are from the Maltsev condition for $SD(\vee)$

Q.E.D.

$\mathbf{A}$: minimal $SD(\vee)$ algebra st. $\exists$ cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant

- The core theorem (Marcin's talk): There exists a nonidentical retraction $f : (A, R) \to (A, R)$, i.e. a mapping $f : A \to A$, $f \neq id$ s.t.
  - $f^2 = f$ (i.e. f is identical on its image)
  - if $(a_1, \ldots, a_p) \in R$, then $(f(a_1), \ldots, f(a_p)) \in R$
- Assume $\mathbf{A} = (A, t_1, \ldots, t_m)$, where $t_1, \ldots, t_m$ are from the Maltsev condition for $SD(\vee)$
- Consider $\mathbf{B} = (f(A), ft_1, \ldots, ft_m)$

Q.E.D.

A: minimal $SD(\vee)$ algebra st. $\exists$ cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant

- The core theorem (Marcin's talk): There exists a nonidentical retraction $f : (A, R) \to (A, R)$, i.e. a mapping $f : A \to A$, $f \neq id$ s.t.
  - $f^2 = f$ (i.e. f is identical on its image)
  - if $(a_1, \ldots, a_p) \in R$, then $(f(a_1), \ldots, f(a_p)) \in R$
- Assume $\mathbf{A} = (A, t_1, \ldots, t_m)$, where $t_1, \ldots, t_m$ are from the Maltsev condition for $SD(\vee)$
- Consider $\mathbf{B} = (f(A), ft_1, \ldots, ft_m)$
  - $|B| < |A|$

Q.E.D.

A: minimal $SD(\vee)$ algebra st. $\exists$ cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant

- The core theorem (Marcin's talk): There exists a nonidentical retraction $f : (A, R) \to (A, R)$, i.e. a mapping $f : A \to A$, $f \neq id$ s.t.
  - $f^2 = f$ (i.e. f is identical on its image)
  - if $(a_1, \dots, a_p) \in R$, then $(f(a_1), \dots, f(a_p)) \in R$
- Assume $\mathbf{A} = (A, t_1, \dots, t_m)$, where $t_1, \dots, t_m$ are from the Maltsev condition for $SD(\vee)$
- Consider $\mathbf{B} = (f(A), ft_1, \dots, ft_m)$
  - $|B| < |A|$
  - **B** is $SD(\vee)$ (as $ft_1, \dots, ft_m$ satisfy all linear equations satisfied by $t_1, \dots, t_m$)

Q.E.D.

$\mathbf{A}$: minimal $SD(\vee)$ algebra st. $\exists$ cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant

- The core theorem (Marcin's talk): There exists a nonidentical retraction $f : (A, R) \to (A, R)$, i.e. a mapping $f : A \to A$, $f \neq id$ s.t.
  - $f^2 = f$ (i.e. f is identical on its image)
  - if $(a_1, \ldots, a_p) \in R$, then $(f(a_1), \ldots, f(a_p)) \in R$
- Assume $\mathbf{A} = (A, t_1, \ldots, t_m)$, where $t_1, \ldots, t_m$ are from the Maltsev condition for $SD(\vee)$
- Consider $\mathbf{B} = (f(A), ft_1, \ldots, ft_m)$
  - $|B| < |A|$
  - $\mathbf{B}$ is $SD(\vee)$ (as $ft_1, \ldots, ft_m$ satisfy all linear equations satisfied by $t_1, \ldots, t_m$)
  - $(\mathbf{R} \cap \mathbf{B}^p) \leq \mathbf{B}^p$ is cyclic, without a constant tuple

Q.E.D.

A: minimal $SD(\vee)$ algebra st. $\exists$ cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant

- The core theorem (Marcin's talk): There exists a nonidentical retraction $f : (A, R) \to (A, R)$, i.e. a mapping $f : A \to A$, $f \neq id$ s.t.
  - $f^2 = f$ (i.e. f is identical on its image)
  - if $(a_1, \ldots, a_p) \in R$, then $(f(a_1), \ldots, f(a_p)) \in R$
- Assume $\mathbf{A} = (A, t_1, \ldots, t_m)$, where $t_1, \ldots, t_m$ are from the Maltsev condition for $SD(\vee)$
- Consider $\mathbf{B} = (f(A), ft_1, \ldots, ft_m)$
  - $|B| < |A|$
  - **B** is $SD(\vee)$ (as $ft_1, \ldots, ft_m$ satisfy all linear equations satisfied by $t_1, \ldots, t_m$)
  - $(\mathbf{R} \cap \mathbf{B}^p) \leq \mathbf{B}^p$ is cyclic, without a constant tuple
  - A contradiction!

Q.E.D.

$\mathbf{A}$: minimal $SD(\vee)$ algebra st. $\exists$ cyclic $\mathbf{R} \leq \mathbf{A}^p$ with no constant

- The core theorem (Marcin's talk): There exists a nonidentical retraction $f : (A, R) \to (A, R)$, i.e. a mapping $f : A \to A$, $f \neq id$ s.t.
  - $f^2 = f$ (i.e. f is identical on its image)
  - if $(a_1, \ldots, a_p) \in R$, then $(f(a_1), \ldots, f(a_p)) \in R$
- Assume $\mathbf{A} = (A, t_1, \ldots, t_m)$, where $t_1, \ldots, t_m$ are from the Maltsev condition for $SD(\vee)$
- Consider $\mathbf{B} = (f(A), ft_1, \ldots, ft_m)$
  - $|B| < |A|$
  - $\mathbf{B}$ is $SD(\vee)$ (as $ft_1, \ldots, ft_m$ satisfy all linear equations satisfied by $t_1, \ldots, t_m$)
  - $(\mathbf{R} \cap \mathbf{B}^p) \leq \mathbf{B}^p$ is cyclic, without a constant tuple
  - A contradiction!
  - Thank you!!!