Jónsson Terms Imply Cyclic Terms For Finite Algebras

Libor Barto, Marcin Kozik, Todd Niven

Charles University in Prague,
Czech Republic

Algorithmic Complexity and Universal Algebra, Szeged 2007

Cyclic terms

DEFINITION n-ary cyclic term = term $t(x_1, \dots, x_n)$ satisfying

- t is idempotent … $t(x, x, \dots, x) \approx x$
- $t(x_1, x_2, \dots, x_n) \approx t(x_2, x_3, \dots, x_n, x_1)$

Cyclic terms

DEFINITION n-ary cyclic term = term $t(x_1, \dots, x_n)$ satisfying

- t is idempotent … $t(x, x, \dots, x) \approx x$
- $t(x_1, x_2, \dots, x_n) \approx t(x_2, x_3, \dots, x_n, x_1)$

FACT "Only primes matter"
Let $\mathbf{A}$ be an algebra.
$C(\mathbf{A}) = \{n \in \omega \mid \mathbf{A}$ has an n-ary cyclic term op.$\}$.
Then $m, n \in C(\mathbf{A})$ iff $mn \in C(\mathbf{A})$.

Cyclic terms

DEFINITION n-ary cyclic term = term $t(x_1, \ldots, x_n)$ satisfying

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

FACT "Only primes matter"
Let $\mathbf{A}$ be an algebra.
$C(\mathbf{A}) = \{n \in \omega \mid \mathbf{A} \text{ has an } n\text{-ary cyclic term op.}\}$.
Then $m, n \in C(\mathbf{A})$ iff $mn \in C(\mathbf{A})$.

PROPOSITION "Semantic meaning"
Let $\mathbb{V}$ be an idempotent variety. $\mathbb{V}$ has n-ary cyclic term iff for all $\mathbf{A} \in \mathbb{V}$ and $\alpha \in \mathrm{Aut}(\mathbf{A})$, if $\alpha^n = id$, then α has a fixed point.

Question: Does majority imply cyclic?

RECALL Majority term

$\ldots m(x,x,y) \approx m(x,y,x) \approx m(y,x,x) \approx x$

Question: Does majority imply cyclic?

RECALL Majority term

$\ldots m(x,x,y) \approx m(x,y,x) \approx m(y,x,x) \approx x$

QUESTION McKenzie 07? Does every finite algebra with a majority term have a cyclic term?

Question: Does majority imply cyclic?

RECALL Majority term

$\ldots m(x,x,y) \approx m(x,y,x) \approx m(y,x,x) \approx x$

QUESTION McKenzie 07? Does every finite algebra with a majority term have a cyclic term?

MOTIVATION Constraint satisfaction problem

Question: Does majority imply cyclic?

RECALL Majority term
$\ldots m(x,x,y) \approx m(x,y,x) \approx m(y,x,x) \approx x$

QUESTION McKenzie 07? Does every finite algebra with a majority term have a cyclic term?

MOTIVATION Constraint satisfaction problem

ANSWER Everyone 07 No!

Question: Does majority imply cyclic?

RECALL Majority term

$\dots m(x, x, y) \approx m(x, y, x) \approx m(y, x, x) \approx x$

QUESTION McKenzie 07? Does every finite algebra with a majority term have a cyclic term?

MOTIVATION Constraint satisfaction problem

ANSWER Kozik, Marković, Computer 07 Yes, for atmost 3-element algebras!

Question: Does majority imply cyclic?

RECALL Majority term

$\ldots m(x,x,y) \approx m(x,y,x) \approx m(y,x,x) \approx x$

QUESTION McKenzie 07? Does every finite algebra with a majority term have a cyclic term?

MOTIVATION Constraint satisfaction problem

ANSWER Barto, Kozik, Niven 07 Yes!

Question: Does majority imply cyclic?

RECALL Majority term

$\dots m(x,x,y) \approx m(x,y,x) \approx m(y,x,x) \approx x$

QUESTION McKenzie 07? Does every finite algebra with a majority term have a cyclic term?

MOTIVATION Constraint satisfaction problem

THEOREM Barto, Kozik, Niven "Majority $\Rightarrow$ many cyclic terms"

Question: Does majority imply cyclic?

RECALL Majority term

$\ldots m(x,x,y) \approx m(x,y,x) \approx m(y,x,x) \approx x$

QUESTION McKenzie 07? Does every finite algebra with a majority term have a cyclic term?

MOTIVATION Constraint satisfaction problem

THEOREM Barto, Kozik, Niven "Majority $\Rightarrow$ many cyclic terms"

Let $\mathbf{A}$ be a finite algebra with a majority term. Then $\mathbf{A}$ has a p-ary cyclic term for every prime $p > |\mathbf{A}|$.

Question: Does majority imply cyclic?

RECALL Majority term

$\ldots m(x,x,y) \approx m(x,y,x) \approx m(y,x,x) \approx x$

QUESTION McKenzie 07? Does every finite algebra with a majority term have a cyclic term?

MOTIVATION Constraint satisfaction problem

THEOREM Barto, Kozik, Niven "Majority $\Rightarrow$ many cyclic terms"

Let $\mathbf{A}$ be a finite algebra with a majority term. Then $\mathbf{A}$ has a p-ary cyclic term for every prime $p > |\mathbf{A}|$. And we can't want more.

Several kinds of terms

- majority (3-NU) $m(y,x,x) \approx m(x,y,x) \approx m(x,x,y) \approx x$

Several kinds of terms

- majority (3-NU) $m(y, x, x) \approx m(x, y, x) \approx m(x, x, y) \approx x$
- n-near unanimity (n-NU) $u(y, x, x, \dots, x) \approx u(x, y, x, x, \dots, x) \approx \cdots \approx u(x, \dots, x, y) \approx x$

Several kinds of terms

- majority (3-NU) $m(y,x,x) \approx m(x,y,x) \approx m(x,x,y) \approx x$
- n-near unanimity (n-NU) $u(y,x,x,\dots,x) \approx u(x,y,x,x,\dots,x) \approx \cdots \approx u(x,\dots,x,y) \approx x$
- n-weak near unanimity (n-WNU) $u(y,x,x,\dots,x) \approx u(x,y,x,x,\dots,x) \approx \cdots \approx u(x,\dots,x,y),\ u(x,\dots,x) \approx x$

Several kinds of terms

- majority (3-NU) $m(y,x,x) \approx m(x,y,x) \approx m(x,x,y) \approx x$
- n-near unanimity (n-NU) $u(y,x,x,\ldots,x) \approx u(x,y,x,x,\ldots,x) \approx \cdots \approx u(x,\ldots,x,y) \approx x$
- n-weak near unanimity (n-WNU) $u(y,x,x,\ldots,x) \approx u(x,y,x,x,\ldots,x) \approx \cdots \approx u(x,\ldots,x,y),\ u(x,\ldots,x) \approx x$
- Malcev (CP) $p(x,x,y) \approx p(y,x,x) \approx y$

Several kinds of terms

- majority (3-NU) $m(y,x,x) \approx m(x,y,x) \approx m(x,x,y) \approx x$
- n-near unanimity (n-NU) $u(y,x,x,\ldots,x) \approx u(x,y,x,x,\ldots,x) \approx \cdots \approx u(x,\ldots,x,y) \approx x$
- n-weak near unanimity (n-WNU) $u(y,x,x,\ldots,x) \approx u(x,y,x,x,\ldots,x) \approx \cdots \approx u(x,\ldots,x,y),\ u(x,\ldots,x) \approx x$
- Malcev (CP) $p(x,x,y) \approx p(y,x,x) \approx y$
- Jónsson (CD)

Several kinds of terms

- majority (3-NU) $m(y, x, x) \approx m(x, y, x) \approx m(x, x, y) \approx x$
- n-near unanimity (n-NU) $u(y, x, x, \dots, x) \approx u(x, y, x, x, \dots, x) \approx \dots \approx u(x, \dots, x, y) \approx x$
- n-weak near unanimity (n-WNU) $u(y, x, x, \dots, x) \approx u(x, y, x, x, \dots, x) \approx \dots \approx u(x, \dots, x, y),\ u(x, \dots, x) \approx x$
- Malcev (CP) $p(x, x, y) \approx p(y, x, x) \approx y$
- Jónsson (CD)
- Gumm (CM)

Several kinds of terms

- majority (3-NU) $m(y,x,x) \approx m(x,y,x) \approx m(x,x,y) \approx x$
- n-near unanimity (n-NU) $u(y,x,x,\dots,x) \approx u(x,y,x,x,\dots,x) \approx \dots \approx u(x,\dots,x,y) \approx x$
- n-weak near unanimity (n-WNU) $u(y,x,x,\dots,x) \approx u(x,y,x,x,\dots,x) \approx \dots \approx u(x,\dots,x,y),\ u(x,\dots,x) \approx x$
- Malcev (CP) $p(x,x,y) \approx p(y,x,x) \approx y$
- Jónsson (CD)
- Gumm (CM)
- Taylors

Look at the blackboard!

FACT 3-NU $\Rightarrow$ 4-NU $\Rightarrow$ 5-NU $\Rightarrow \ldots \Rightarrow$ Jónsson $\Rightarrow$ Gumm $\Rightarrow$ Taylor (the weakest nontrivial), Malcev $\Rightarrow$ Gumm

THEOREM Maróti, McKenzie 06 For a finite algebra, Taylor $\Rightarrow$ WNU.

THEOREMS For a finite algebra

- Jónsson $\Rightarrow$ many cyclic terms BKN
- Malcev $\Rightarrow$ many cyclic terms Maróti, McKenzie
- Gumm $\Rightarrow$ many cyclic terms Maróti, McKenzie

QUESTION WNU $\Rightarrow$ (many) cyclic term(s)? (For finite algebras, of course)

I'll sketch the proof of

THEOREM Let **A** be a finite algebra with Jónsson term operations. Then **A** has a p-ary cyclic term operation for every prime $p > |\mathbf{A}|$.

Proof - the beginning

NOTATION For a tuple $\bar{a} = \langle a_1, \dots, a_n \rangle$, let $\sigma(\bar{a}) = \langle a_2, \dots, a_n, a_1 \rangle$.

Proof - the beginning

NOTATION For a tuple $\bar{a} = \langle a_1, \ldots, a_n \rangle$, let $\sigma(\bar{a}) = \langle a_2, \ldots, a_n, a_1 \rangle$.

FACT Let **A** be a finite idempotent algebra, $n \geq 2$ be a natural number. TFAE

Proof - the beginning

NOTATION For a tuple $\bar{a} = \langle a_1, \ldots, a_n \rangle$, let $\sigma(\bar{a}) = \langle a_2, \ldots, a_n, a_1 \rangle$.

FACT Let **A** be a finite idempotent algebra, $n \geq 2$ be a natural number. TFAE

- **A** has n-ary cyclic term.

Proof - the beginning

NOTATION For a tuple $\bar{a} = \langle a_1, \ldots, a_n \rangle$, let $\sigma(\bar{a}) = \langle a_2, \ldots, a_n, a_1 \rangle$.

FACT Let $\mathbf{A}$ be a finite idempotent algebra, $n \geq 2$ be a natural number. TFAE

- $\mathbf{A}$ has n-ary cyclic term.
- $(\exists t$ n-ary term $)$ $(\forall \bar{a} \in \mathbf{A}^n)$ $t(\bar{a}, \sigma(\bar{a}), \sigma^2(\bar{a}), \ldots, \sigma^{n-1}(\bar{a})) = \langle c, c, \ldots, c \rangle$ for some $c \in \mathbf{A}$.

Proof - the beginning

NOTATION For a tuple $\bar{a} = \langle a_1, \ldots, a_n \rangle$, let $\sigma(\bar{a}) = \langle a_2, \ldots, a_n, a_1 \rangle$.

FACT Let $\mathbf{A}$ be a finite idempotent algebra, $n \geq 2$ be a natural number. TFAE

- $\mathbf{A}$ has n-ary cyclic term.
- $(\exists t \ n\text{-ary term }) \ (\forall \bar{a} \in \mathbf{A}^n)$ $t(\bar{a}, \sigma(\bar{a}), \sigma^2(\bar{a}), \ldots, \sigma^{n-1}(\bar{a})) = \langle c, c, \ldots, c \rangle$ for some $c \in \mathbf{A}$.
- $(\forall \bar{a} \in \mathbf{A}^n) \ (\exists t \ n\text{-ary term })$ $t(\bar{a}, \sigma(\bar{a}), \sigma^2(\bar{a}), \ldots, \sigma^{n-1}(\bar{a})) = \langle c, c, \ldots, c \rangle$ for some $c \in \mathbf{A}$.

Proof - the beginning

NOTATION For a tuple $\bar{a} = \langle a_1, \ldots, a_n \rangle$, let $\sigma(\bar{a}) = \langle a_2, \ldots, a_n, a_1 \rangle$.

FACT Let $\mathbf{A}$ be a finite idempotent algebra, $n \geq 2$ be a natural number. TFAE

- $\mathbf{A}$ has n-ary cyclic term.
- $(\exists t \ n\text{-ary term }) \ (\forall \bar{a} \in \mathbf{A}^n)$ $t(\bar{a}, \sigma(\bar{a}), \sigma^2(\bar{a}), \ldots, \sigma^{n-1}(\bar{a})) = \langle c, c, \ldots, c \rangle$ for some $c \in \mathbf{A}$.
- $(\forall \bar{a} \in \mathbf{A}^n) \ \ (\exists t \ n\text{-ary term })$ $t(\bar{a}, \sigma(\bar{a}), \sigma^2(\bar{a}), \ldots, \sigma^{n-1}(\bar{a})) = \langle c, c, \ldots, c \rangle$ for some $c \in \mathbf{A}$.
- $(\forall \bar{a} \in \mathbf{A}^n) \ Sg(\bar{a}, \sigma(\bar{a}), \ldots) \ni \langle c, c \ldots, c \rangle$.

Proof - the beginning

NOTATION For a tuple $\bar{a} = \langle a_1, \dots, a_n \rangle$, let $\sigma(\bar{a}) = \langle a_2, \dots, a_n, a_1 \rangle$.

FACT Let $\mathbf{A}$ be a finite idempotent algebra, $n \geq 2$ be a natural number. TFAE

- $\mathbf{A}$ has n-ary cyclic term.
- $(\exists t \ n\text{-ary term}) \ (\forall \bar{a} \in \mathbf{A}^n)$ $t(\bar{a}, \sigma(\bar{a}), \sigma^2(\bar{a}), \dots, \sigma^{n-1}(\bar{a})) = \langle c, c, \dots, c \rangle$ for some $c \in \mathbf{A}$.
- $(\forall \bar{a} \in \mathbf{A}^n) \ (\exists t \ n\text{-ary term})$ $t(\bar{a}, \sigma(\bar{a}), \sigma^2(\bar{a}), \dots, \sigma^{n-1}(\bar{a})) = \langle c, c, \dots, c \rangle$ for some $c \in \mathbf{A}$.
- $(\forall \bar{a} \in \mathbf{A}^n) \ Sg(\bar{a}, \sigma(\bar{a}), \dots) \ni \langle c, c \dots, c \rangle$.
- Every $S \leq \mathbf{A}^n$, $\sigma(S) = S$ contains a constant n-tuple.

First part of the proof - loops in graphs

LEMMA Let $G \leq \mathbf{B}^2$, where $\mathbf{B}$ has a majority term. Let G (viewed as a graph) be strongly connected and the greatest common divisor of the lengths of cycles in G is 1.
Then G cotains a loop.

First part of the proof - loops in graphs

LEMMA Let $G \leq \mathbf{B}^2$, where $\mathbf{B}$ has a majority term. Let G (viewed as a graph) be strongly connected and the greatest common divisor of the lengths of cycles in G is 1.
Then G cotains a loop.

Crucial idea of the proof:
Consider the following system of sets

$$\mathcal{C}_G = \{R \subseteq A \,|\, (\forall r, s \in R,\ a \in A) \quad \begin{array}{l} m(r,s,a) \in R \\ m(r,a,s) \in R \\ m(a,r,s) \in R\} \end{array}$$

First part of the proof - loops in graphs

LEMMA Let $G \leq \mathbf{B}^2$, where $\mathbf{B}$ has a majority term. Let G (viewed as a graph) be strongly connected and the greatest common divisor of the lengths of cycles in G is 1.
Then G cotains a loop.

Crucial idea of the proof:
Consider the following system of sets

$$\begin{aligned}\mathcal{C}_G = \{R \subseteq A \,|\, (\forall r, s \in R,\ a \in A) \quad & m(r,s,a) \in R \\ & m(r,a,s) \in R \\ & m(a,r,s) \in R\}\end{aligned}$$

It is closed under intersection, it contains singletons, ...

The second part of the proof

Let $\mathbf{A}$ be a minimal counterexample to the theorem wrt $|A|$.

The second part of the proof

Let **A** be a minimal counterexample to the theorem wrt $|A|$.

$\Rightarrow$ **A** is simple.

The second part of the proof

Let **A** be a minimal counterexample to the theorem wrt $|A|$.

$\Rightarrow$ **A** is simple.

Take $S \leq \mathbf{A}^p$, $\sigma(S) = S$ and some $1 \leq k < n$.

The second part of the proof

Let **A** be a minimal counterexample to the theorem wrt $|A|$.

$\Rightarrow$ **A** is simple.

Take $S \leq \mathbf{A}^p$, $\sigma(S) = S$ and some $1 \leq k < n$.

Let $\mathbf{B} = \{\langle a_1, \ldots, a_k \rangle \mid \langle a_1, \ldots, a_p \rangle \in S\} \leq \mathbf{A}^k$

The second part of the proof

Let **A** be a minimal counterexample to the theorem wrt $|A|$.

$\Rightarrow$ **A** is simple.

Take $S \leq \mathbf{A}^p$, $\sigma(S) = S$ and some $1 \leq k < n$.

Let $\mathbf{B} = \{\langle a_1, \ldots, a_k\rangle \mid \langle a_1, \ldots, a_p\rangle \in S\} \leq \mathbf{A}^k$

and $G = \{\langle\ \langle a_1, \ldots, a_k\rangle,\ \langle a_2, \ldots a_{k+1}\rangle\ \rangle \mid \langle a_1, \ldots, a_p\rangle \in S\} \leq \mathbf{B}^2$

The second part of the proof

Let $\mathbf{A}$ be a minimal counterexample to the theorem wrt $|A|$.

$\Rightarrow$ $\mathbf{A}$ is simple.

Take $S \leq \mathbf{A}^p$, $\sigma(S) = S$ and some $1 \leq k < n$.

Let $\mathbf{B} = \{\langle a_1, \ldots, a_k \rangle \mid \langle a_1, \ldots, a_p \rangle \in S\} \leq \mathbf{A}^k$

and $G = \{\langle\ \langle a_1, \ldots, a_k \rangle,\ \langle a_2, \ldots a_{k+1} \rangle\ \rangle \mid \langle a_1, \ldots, a_p \rangle \in S\} \leq \mathbf{B}^2$

- This graph is strongly connected

The second part of the proof

Let $\mathbf{A}$ be a minimal counterexample to the theorem wrt $|A|$.

$\Rightarrow$ $\mathbf{A}$ is simple.

Take $S \leq \mathbf{A}^p$, $\sigma(S) = S$ and some $1 \leq k < n$.

Let $\mathbf{B} = \{\langle a_1, \ldots, a_k \rangle \mid \langle a_1, \ldots, a_p \rangle \in S\} \leq \mathbf{A}^k$

and $G = \{\langle\ \langle a_1, \ldots, a_k \rangle,\ \langle a_2, \ldots a_{k+1} \rangle\ \rangle \mid \langle a_1, \ldots, a_p \rangle \in S\} \leq \mathbf{B}^2$

- This graph is strongly connected
- Every vertex is in a p-cycle

The second part of the proof

Let **A** be a minimal counterexample to the theorem wrt $|A|$.

$\Rightarrow$ **A** is simple.

Take $S \leq \mathbf{A}^p$, $\sigma(S) = S$ and some $1 \leq k < n$.

Let $\mathbf{B} = \{\langle a_1, \dots, a_k \rangle \mid \langle a_1, \dots, a_p \rangle \in S\} \leq \mathbf{A}^k$

and $G = \{\langle\ \langle a_1, \dots, a_k \rangle,\ \langle a_2, \dots a_{k+1} \rangle\ \rangle \mid \langle a_1, \dots, a_p \rangle \in S\} \leq \mathbf{B}^2$

- This graph is strongly connected
- Every vertex is in a p-cycle
- Using simplicity and congruence properties (join semidistributivity suffices) one can find $(lp+1)$-cycle

The second part of the proof

Let **A** be a minimal counterexample to the theorem wrt $|A|$.

$\Rightarrow$ **A** is simple.

Take $S \leq \mathbf{A}^p$, $\sigma(S) = S$ and some $1 \leq k < n$.

Let $\mathbf{B} = \{\langle a_1, \ldots, a_k \rangle \mid \langle a_1, \ldots, a_p \rangle \in S\} \leq \mathbf{A}^k$

and $G = \{\langle\ \langle a_1, \ldots, a_k \rangle,\ \langle a_2, \ldots a_{k+1} \rangle\ \rangle \mid \langle a_1, \ldots, a_p \rangle \in S\} \leq \mathbf{B}^2$

- This graph is strongly connected
- Every vertex is in a p-cycle
- Using simplicity and congruence properties (join semidistributivity suffices) one can find $(lp + 1)$-cycle
- From Lemma we get that it contains loop

The second part of the proof

Let $\mathbf{A}$ be a minimal counterexample to the theorem wrt $|A|$.

$\Rightarrow$ $\mathbf{A}$ is simple.

Take $S \leq \mathbf{A}^p$, $\sigma(S) = S$ and some $1 \leq k < n$.

Let $\mathbf{B} = \{\langle a_1, \dots, a_k\rangle \mid \langle a_1, \dots, a_p\rangle \in S\} \leq \mathbf{A}^k$

and $G = \{\langle\ \langle a_1, \dots, a_k\rangle,\ \langle a_2, \dots a_{k+1}\rangle\ \rangle \mid \langle a_1, \dots, a_p\rangle \in S\} \leq \mathbf{B}^2$

- This graph is strongly connected
- Every vertex is in a p-cycle
- Using simplicity and congruence properties (join semidistributivity suffices) one can find $(lp+1)$-cycle
- From Lemma we get that it contains loop
- If $k = n - 1$ we get a constant tuple

web: http://www.karlin.mff.cuni.cz/$\sim$barto

Thank you for your attention!