Cyclic terms for SD(∨) varieties – revisited

Libor Barto and Marcin Kozik

February 10, 2009

Abstract

We present a direct proof showing that every finite algebra generating a congruence join semidistributive variety has a cyclic term.

1 Introduction

Authors in [1] provide motivation for investigating cyclic terms and an overview of their applicability to the questions connected with the Constraint Satisfaction Problem. It is mentioned there that combining the results of [2], [5] and using theorems from [1] one can show that if a finite algebra generates a congruence join semidistributive variety then it has cyclic terms. In this paper we present a new and direct proof of this fact. The proof links properties of relational structures with an existence of cyclic terms and shows that the connection between relational structures and the structure of algebras associated with them needs further investigation.

2 Preliminaries

Recall that a lattice L is *join semidistributive*, or SD(∨) for short, if $\alpha\vee\beta=\alpha\vee\gamma$ implies $\alpha\vee(\beta\wedge\gamma)=\alpha\vee\beta$ for every $\alpha,\beta,\gamma\in L$. A variety $\mathcal{V}$ is congruence join semidistributive (SD(∨)), if all the algebras in $\mathcal{V}$ have join semidistributive congruence lattices. Equivalently, using results of [3, Theorem 9.11] and [4], a locally finite variety is SD(∨) iff it omits types 1,2 and 5.

A relational structure is a *core*, if every its endomorphism is a bijection. An endomorphism f of a relational structure is a *retraction* if f is identical on its image; and if a relational structure is not a core then it has a retraction onto its proper substructure.

In this paper we use basic results and definitions connected with cyclic terms which can be found in [1]; all relational structures and algebras are finite and we use the convention $p=\{0,1,\dots,p-1\}$.

3 Cyclic subalgebras

We recall a definition of a cyclic relation.

Definition 1. *A relation $R\subseteq A^n$ is* cyclic*, if $(a_0,\dots,a_{n-1})\in R$ implies $(a_1,\dots,a_{n-1},a_0)\in R$ for every $a_0,\dots,a_{n-1}\in A$. A subalgebra of $\mathbf{A}^n$ is* cyclic *if its underlying set is a cyclic relation.*

The remaining part of this section is devoted to a proof of the following theorem:

Theorem 2. *Let* $\mathbf{A}$ *be a finite simple algebra from an SD(*$\vee$*) variety, let* p *be a prime number greater than* $|A|$ *and let* $\mathbf{R} \leq \mathbf{A}^p$ *be a cyclic subalgebra of* $\mathbf{A}^p$*. If* R *has more than one element then the relational structure* (A, R) *is not a core.*

Striving for a contradiction, let us assume that the algebras $\mathbf{A}$ and $\mathbf{R}$ constitute a minimal (with respect to $|A|$) counterexample to the theorem. Then $|R| > 1$ and (A, R) is a core. Moreover it is readily seen that R is a subdirect subalgebra of $\mathbf{A}^p$ and that R doesn't contain a constant tuple.

We will consider a certain subalgebra of a power of $\mathbf{A}$, which we introduce in the following definition.

Definition 3. *By an* unfolding *of a* p*-ary relation* R *over* A *we mean the* p*-ary relation* R' *on the set* $A \times p$ *defined by*

$$R' = \big\{\big((a_0, 0), \ldots, (a_{p-1}, p-1)\big) \in (A \times p)^p \mid (a_0, \ldots, a_{p-1}) \in R\big\}.$$

By an unfolding power *of* R *we mean the subset of* $A^{A\times p}$ *consisting of all the homomorphisms from the relational structure* $(A \times p, R')$ *to* (A, R)*.*

It is easy to see that the set of homomorphisms from $(A \times p, R')$ to (A, R) is a subuniverse of $\mathbf{A}^{A\times p}$. We will denote by $\mathbf{C}$ the algebra with the underlying set equal to the unfolding of R and the operations inherited from $\mathbf{A}^{A\times p}$. It is helpful to write an element $g \in C$ as a p-tuple $(f_0, \ldots, f_{p-1})$ of mappings from A to A, namely $f_i(a) = g((a, i))$ for all $i < p$, $a \in A$. The condition that g is a homomorphism from $(A \times p, R')$ to (A, R) translates into the condition

$$(f_0(a_0), f_1(a_1), \ldots, f_{p-1}(a_{p-1})) \in R \text{ whenever } (a_0, \ldots, a_{p-1}) \in R.$$

We summarize trivial consequences of the definitions in a single fact:

Fact 4.

- $(\mathrm{id}_A, \mathrm{id}_A, \ldots, \mathrm{id}_A) \in C$*;*
- $\mathrm{const}(\mathbf{a}) = (\mathrm{const}(a_0), \ldots, \mathrm{const}(a_{p-1})) \in C$ *iff* $\mathbf{a} = (a_0, \ldots, a_{p-1}) \in R$*, where* $\mathrm{const}(a)$ *denotes the constant mapping with image* $\{a\}$*;*
- *if* $(f, f, \ldots, f) \in C$ *then* f *is an endomorphism of the relational structure* (A, R)*;*
- *if* $c = (f_0, \ldots, f_{p-1})$*,* $d = (g_0, \ldots, g_{p-1}) \in C$*, then* $c \circ d = (f_0 \circ g_0, \ldots, f_{p-1} \circ g_{p-1}) \in C$*, where* $\circ$ *denotes the composition of functions;*
- *if* $(f_0, \ldots, f_{p-1}) \in C$ *then, for any* j*,* $(f_j, f_{j+1}, \ldots, f_{j+p-1}) \in C$*, where the indices are computed modulo* p *(since* R *is a cyclic relation).*

In the algebra $\mathbf{R}$ we denote by π_i the kernel of the i-th projection of $\mathbf{R} \leq \mathbf{A}^p$. Moreover for any $a \in A$ and any $i < p$ we define a congruence $\sim_{(a,i)}$ on $\mathbf{C}$ by putting $(f_0, \ldots, f_{p-1}) \sim_{(a,i)} (f'_0, \ldots, f'_{p-1})$ iff $f_i(a) = f'_i(a)$ (it is the kernel of the projection of $\mathbf{C} \leq \mathbf{A}^{A\times p}$ to the (a, i)-th coordinate).

Claim 1. *Let* $i < j < p$*. Then*[1] $\pi_i \vee \pi_j = 1_{\mathbf{R}}$*.*

[1] The full congruence of an algebra $\mathbf{X}$ is denoted by $1_{\mathbf{X}}$ and the smallest one by $0_{\mathbf{X}}$.

Proof. We'll first prove that $\pi_i \neq \pi_j$ for any $i < j < p$. Suppose, for the contrary, that $\pi_i = \pi_j$ for some $i < j$. Then, for any $\mathbf{a}, \mathbf{b} \in R$, we have $a_i = b_i$ iff $a_j = b_j$ and, by cyclicity of R, $a_k = b_k$ iff $a_{j-i+k} = b_{j-i+k}$ for any k (where the indices are computed modulo p). Further $a_k = b_k$ implies $a_{(j-i)l+k} = b_{(j-i)l+k}$ for any k, l and the choice of p provides $\pi_0 = \pi_1 = \cdots = \pi_{p-1}$. Since $\bigwedge_{i<p} \pi_i = 0_{\mathbf{R}}$ we obtain $\pi_i = 0_{\mathbf{R}}$ for all i. Take any tuple $\mathbf{a} \in R$. Since $p > |A|$, two coordinates of $\mathbf{a}$ must be equal, say $a_i = a_j$ for some $i < j$, and therefore $(a_i, a_{i+1}, \ldots, a_{i+p-1})\ \pi_0\ (a_j, a_{j+1}, \ldots, a_{j+p-1})$. This implies that $a_{i+k} = a_{j+k}$ for all $k < p$, thus, by the primality of p, $\mathbf{a}$ is a constant tuple – this contradiction proves that $\pi_i \neq \pi_j$.

Since $\pi_i \neq \pi_j$ we can assume, without loss of generality, that there exist tuples $\mathbf{a}, \mathbf{b}$ in R such that $a_i = b_i$ and $a_j \neq b_j$. Therefore the congruence ρ on $\mathbf{A}$ defined as

$$a\, \rho\, a' \text{ iff } \exists\, \mathbf{a}, \mathbf{a}' \in R \text{ such that } a_j = a, a'_j = a' \text{ and } \mathbf{a}\, \pi_i\, \mathbf{b}$$

is greater than $0_{\mathbf{A}}$ and, since $\mathbf{A}$ is simple, $\rho = 1_{\mathbf{A}}$ and therefore $\pi_i \vee \pi_j = 1_{\mathbf{R}}$. □

Claim 2. *Let $a, b \in A$ and let $i \neq j$. Then $\sim_{(a,i)} \vee \sim_{(b,j)} = 1_{\mathbf{C}}$.*

Proof. Let h, g be arbitrary elements of $\mathbf{C}$. As R is subdirect, there exist elements $\mathbf{c}, \mathbf{d} \in R$ such that $h \sim_{(a,i)} \mathrm{const}(\mathbf{c})$ and $g \sim_{(a,i)} \mathrm{const}(\mathbf{d})$. Since $\pi_i \vee \pi_j$ is the full congruence on $\mathbf{R}$ (by the last claim) there is a chain of elements $\mathbf{c} = \mathbf{c}_0, \ldots, \mathbf{c}_m = \mathbf{d}$ such that for any l we have $\mathbf{c}_l\ \pi_i\ \mathbf{c}_{l+1}$ or $\mathbf{c}_l\ \pi_j\ \mathbf{c}_{l+1}$. Then $\mathrm{const}(\mathbf{c}_0), \ldots, \mathrm{const}(\mathbf{c}_m)$ is the chain connecting $\mathrm{const}(\mathbf{c})$ to $\mathrm{const}(\mathbf{d})$ in $\sim_{(a,i)} \vee \sim_{(b,j)}$ and the claim is proved. □

We introduce an auxiliary notation: for $i < p$ we put

$$\eta_i = \bigwedge_{j \neq i, a \in A} \sim_{(a,j)},$$

and proceed to the next claim.

Claim 3. $\bigvee_{i<p} \eta_i = 1_{\mathbf{C}}$.

Proof. Let $b \in A, i < p$ be arbitrary. Fro every $a \in A$ and $j < p$ such that $i \neq j$ we have $\sim_{(b,i)} \vee \sim_{(a,j)} = 1_{\mathbf{C}}$. Congruence lattice of $\mathbf{C}$ is SD($\vee$), therefore $\sim_{(b,i)} \vee \eta_i = 1_{\mathbf{C}}$. It follows that for every $b \in A$, $k \neq 0$ we have

$$\sim_{(b,k)} \vee \bigvee_{0<i<p} \eta_i = 1_{\mathbf{C}}.$$

Using the SD($\vee$) property again we obtain

$$\bigwedge_{k \neq 0, b \in A} \sim_{(b,k)} \vee \bigvee_{0<i<p} \eta_i = 1_{\mathbf{C}},$$

and we are done. □

Take any $\mathbf{a} \in R$. The last claim implies that

$$(\mathrm{id}_A, \ldots, \mathrm{id}_A) \bigvee_{i<p} \eta_i\ \mathrm{const}(\mathbf{a}),$$

therefore there exist a natural number n, numbers $m_i < p$, $i < n$ and elements $\mathbf{f}^i = (f^i_0, \dots, f^i_{p-1})$, $i \leq n$ in C such that

$$(\mathrm{id}_A, \dots, \mathrm{id}_A) = \mathbf{f}^0 \ \eta_{m_0} \ \mathbf{f}^1 \ \eta_{m_1} \ \mathbf{f}^2 \ \eta_{m_2} \ \dots \ \eta_{m_{n-1}} \ \mathbf{f}^m = \mathrm{const}(\mathbf{a}).$$

Let j be the first index such that f^{j+1}_k is not a bijection for some $k < p$. Since $\mathbf{f}^j = (f^j_0, \dots, f^j_{p-1}) \ \eta_{m_j} \ (f^{j+1}_0, \dots, f^{j+1}_{p-1}) = \mathbf{f}^{j+1}$, we know that $f^j_l = f^{j+1}_l$ for all $l \neq m_j$. Thus, putting $k = m_j$, f^{j+1}_k is not a bijection, while f^{j+1}_l is a bijection for all $l \neq k$.

By composing $\mathbf{f}^{j+1}$ enough many times with itself, we obtain a tuple

$$(\mathrm{id}_A, \dots, \mathrm{id}_A, g, \mathrm{id}_A, \dots, \mathrm{id}_A)$$

in C, where g is on the k-th position and g is not a bijection. From Fact 4 it follows that all the tuples

$$(g, \mathrm{id}_A, \dots, \mathrm{id}_A), (\mathrm{id}_A, g, \mathrm{id}_A, \dots, \mathrm{id}_A), \dots, (\mathrm{id}_A, \dots, \mathrm{id}_A, g)$$

are in C, therefore their composition – the tuple $(g, g, \dots, g)$ – is in C as well. Then, again from Fact 4, g is an endomorphism of the relational structure (A, B) which is not a bijection. This contradiction concludes the proof of Theorem 2.

4 Cyclic terms exist

We begin with a definition:

Definition 5. *A variety of algebras $\mathcal{V}$ is* linear *if it is axiomatized by* linear identities *i.e. identities with no nested terms.*

It is known [3, Theorem 9.11] and [4] that there exists a sequence of linear varieties, which we denote by $\mathcal{J}_\mathrm{n}$, such that an algebra $\mathbf{A}$ is in a congruence join semidistributive variety iff $\mathbf{A}$ has a reduct in $\mathcal{J}_\mathrm{n}$.

Definition 6. *A relational structure is* $\mathcal{V}$-compatible *(for a variety $\mathcal{V}$) if the algebra of all compatible operations has a reduct in $\mathcal{V}$.*

An easy proposition follows.

Proposition 7. *Let $\mathcal{V}$ be a linear variety and let $\mathbf{R}$ be a $\mathcal{V}$-compatible relational structure. Then all retracts of $\mathbf{R}$ are also $\mathcal{V}$-compatible.*

Proof. Let $\mathcal{V}$ and $\mathbf{R}$ be as in the statement of the theorem and let h be a retraction of $\mathbf{R}$ onto a relational structure $\mathbf{S}$. For any compatible operation $f(x_0, \dots, x_{n-1})$ of $\mathbf{R}$, the function $f'(x_0, \dots, x_{n-1}) = h(f(x_0, \dots, x_{n-1}))$ is compatible with $\mathbf{S}$ (and with $\mathbf{R}$ as well). Moreover a linear identity remains true when we substitute all the terms with their primed versions. This proves that $\mathbf{S}$ is $\mathcal{V}$-compatible. □

The last ingredients for the main result are the following facts from [1] (Lemma 2.4 and Lemma 2.5).

Fact 8. *Let $\mathbf{A}$ be an idempotent algebra and let $n \geq 2$ be a natural number.*

- $\mathbf{A}$ *has a cyclic term of arity* n *iff every cyclic subalgebra of* $\mathbf{A}^n$ *contains a constant tuple.*
- *If there exists a congruence* α *of* $\mathbf{A}$ *such that* $\mathbf{A}/\alpha$ *as well as all* α *classes have a cyclic term of arity* n*, then* $\mathbf{A}$ *has a cyclic term of arity* n*.*

Now we are ready to prove the main theorem:

Theorem 9. *Let* $\mathbf{A}$ *be a finite algebra in a congruence join semidistributive variety. Then for any prime* p *greater than* $|A|$ *the algebra* $\mathbf{A}$ *has a cyclic term of arity* p*.*

Striving for a contradiction, we take a minimal counterexample with respect to $\mathbf{A}$. We can assume that $\mathbf{A}$ is idempotent, otherwise we can replace $\mathbf{A}$ by its idempotent reduct. From Fact 8 we know that $\mathbf{A}$ is simple and there exists a cyclic subuniverse R of $\mathbf{A}^p$ with no constant tuple. Clearly R can't have just one element, therefore, by Theorem 2, there is a retraction of the relational structure (A, R) onto a substructure (A', R'), where $|A'| < |A|$. Since, for some n, (A, R) is $\mathcal{J}_{\mathrm{n}}$-compatible, then, by Proposition 7, (A', R') is $\mathcal{J}_{\mathrm{n}}$-compatible as well. As (A', R') is a retraction of (A, R) and R is cyclic, R' is cyclic too. Using Fact 8 and minimality of $\mathbf{A}$ we get that R' contains a constant tuple. But $R' \subset R$, which implies that R contains a constant tuple, a contradiction.

References

[1] Libor Barto, Marcin Kozik, Miklós Maróti, Ralph McKenzie, and Todd Niven. Congruence modularity implies cyclic terms for finite algebras. Algebra Universalis (to appear), 2007.

[2] Libor Barto, Marcin Kozik, and Todd Niven. The CSP dichotomy holds for digraphs with no sources and no sinks (a positive answer to a conjecture of Bang-Jensen and Hell). *SIAM Journal on Computing*, 38(5):1782–1802, 2009.

[3] David Hobby and Ralph McKenzie. *The structure of finite algebras*, volume 76 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 1988.

[4] Keith A. Kearnes. Congruence join semidistributivity is equivalent to a congruence identity. *Algebra Universalis*, 46(3):373–387, 2001.

[5] Miklós Maróti and Ralph McKenzie. Existence theorems for weakly symmetric operations. Algebra Universalis (to appear), 2007.