Cyclic terms for $SD_{\vee}$ varieties revisited

LIBOR BARTO AND MARCIN KOZIK

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

1. Introduction

The authors of [1] provide motivation for investigating cyclic terms and an overview of their applicability to questions connected with the Constraint Satisfaction Problem. It is mentioned there that combining the results of [2] and [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 $SD_{\vee}$ 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* ($SD_{\vee}$), 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 $SD_{\vee}$ iff it omits types **1**, **2** and **5**.

A relational structure is a *core* if every one of its endomorphisms is a bijection. An endomorphism f of a relational structure is a *retraction* if f is identical on its image; if a relational structure is not a core, then it has a retraction onto a 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 assumed to be finite, and we use the convention $p = \{0, 1, \dots, p-1\}$.

Presented by E. Kiss.

Received February 10, 2009; accepted in final form September 16, 2009.

The first author was supported by the Grant Agency of the Czech Republic under the grant No. 201/09/P223 and by the Ministry of Education of the Czech Republic under the grants No. MEB 050817 and No. MSM 0021620839. The second author thanks the Foundation for Polish Science grant No. HOM/2008/7 (supported by MF EOG), Eduard Čech Center grant No. LC 505 and Ministry of Science and Higher Education of Poland grant No. N206 357036.

3. Cyclic subalgebras

We recall the definition of a cyclic relation.

Definition 3.1. 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 3.2. *Let $\mathbf{A}$ be a finite simple algebra from an $\text{SD}_\vee$ variety, let p be a prime number greater than $|A|$ and let $\mathbf{R} \leq \mathbf{A}^p$ be a cyclic and subdirect subalgebra of $\mathbf{A}^p$. If A 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 $|A| > 1$, (A, R) is a core, and it is readily seen 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 3.3. 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

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

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 power 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 $(f_0, \dots, f_{p-1})$ of mappings from A to A , namely $f_i(a) = g((a, i))$ for all $i < p$ and $a \in A$. The condition that g is a homomorphism from $(A \times p, R')$ to (A, R) translates into the condition that

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

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

Fact 3.4.

- $(\text{id}_A, \text{id}_A, \dots, \text{id}_A) \in C$;
- $\text{const}(\mathbf{a}) = (\text{const}(a_0), \dots, \text{const}(a_{p-1})) \in C$ iff $\mathbf{a} = (a_0, \dots, a_{p-1}) \in R$, where $\text{const}(a)$ denotes the constant mapping with image $\{a\}$;
- if $(f, f, \dots, f) \in C$, then f is an endomorphism of the relational structure (A, R) ;

- if $c = (f_0, \dots, f_{p-1})$ and $d = (g_0, \dots, g_{p-1}) \in C$, then we have $c \circ d = (f_0 \circ g_0, \dots, f_{p-1} \circ g_{p-1}) \in C$, where $\circ$ denotes the composition of functions;
- if $(f_0, \dots, f_{p-1}) \in C$, then for any j we have $(f_j, f_{j+1}, \dots, f_{j+p-1}) \in C$, 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 $(f_0, \dots, f_{p-1}) \sim_{(a,i)} (f'_0, \dots, f'_{p-1})$ 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). The largest congruence of an algebra $\mathbf{R}$ is denoted by $1_{\mathbf{R}}$ and the smallest by $0_{\mathbf{R}}$.

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

Proof. We'll first prove that $\pi_i \neq \pi_j$ for any $i < j < p$. Suppose, to 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 the 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, since p is prime, we get that $\pi_0 = \pi_1 = \dots = \pi_{p-1}$. 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 $(a_i, a_{i+1}, \dots, a_{i+p-1}) \pi_0 (a_j, a_{j+1}, \dots, a_{j+p-1})$. 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 compatible relation 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, the transitive closure of ρ is equal to $1_{\mathbf{A}}$. Thus $\pi_i \vee \pi_j = 1_{\mathbf{R}}$. $\square$

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 $h \sim_{(a,i)} \text{const}(\mathbf{c})$ and $g \sim_{(a,i)} \text{const}(\mathbf{d})$. Since $\pi_i \vee \pi_j$ is the full congruence on $\mathbf{R}$ (by the last claim) there is a chain of elements $\mathbf{c} = \mathbf{c}_0, \dots, \mathbf{c}_m = \mathbf{d}$ 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 $\text{const}(\mathbf{c}_0), \dots, \text{const}(\mathbf{c}_m)$ is the chain connecting $\text{const}(\mathbf{c})$ to $\text{const}(\mathbf{d})$ in $\sim_{(a,i)} \vee \sim_{(b,j)}$ and the claim is proved. $\square$

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

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

Using the $\text{SD}_\vee$ 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. $\square$

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

$$(\text{id}_A, \dots, \text{id}_A) \bigvee_{i < p} \eta_i \text{const}(\mathbf{a});$$

therefore there exist a natural number n , numbers $m_i < p$ for $i < n$, and elements $\mathbf{f}^i = (f_0^i, \dots, f_{p-1}^i)$, where $i \leq n$, in C such that

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

Let j be the first index such that f_k^{j+1} is not a bijection, for some $k < p$. Since $\mathbf{f}^j = (f_0^j, \dots, f_{p-1}^j) \eta_{m_j} (f_0^{j+1}, \dots, f_{p-1}^{j+1}) = \mathbf{f}^{j+1}$, we know that $f_l^j = f_l^{j+1}$ for all $l \neq m_j$. Thus, putting $k = m_j$, f_k^{j+1} is not a bijection, while f_l^{j+1} is a bijection for all $l \neq k$.

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

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

in C , where g is on the k -th position and g is not a bijection. From Fact 3.4, it follows that all the tuples

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

are in C ; therefore their composition – the tuple $(g, g, \dots, g)$ – is in C as well. Then, again from Fact 3.4, g is an endomorphism of the relational structure (A, R) , which is not a bijection. This contradiction concludes the proof of Theorem 3.2.

4. Cyclic terms exist

We begin with a definition:

Definition 4.1. A variety $\mathcal{V}$ of algebras 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 $\mathcal{J}_n$, such that an algebra $\mathbf{A}$ is in a congruence join semidistributive variety iff $\mathbf{A}$ has a reduct in $\mathcal{J}_n$.

Definition 4.2. 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 4.3. *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 proposition, 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 terms with their primed versions. This proves that $\mathbf{S}$ is $\mathcal{V}$ -compatible. $\square$

The last ingredient for the main result is the following fact from [1] (Lemma 2.4 and Lemma 2.5).

Fact 4.4. *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 cyclic terms of arity n , then $\mathbf{A}$ has a cyclic term of arity n .*

Now we are ready to prove the main theorem:

Theorem 4.5. *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 $|A|$. We can assume that $\mathbf{A}$ is idempotent; otherwise we can replace $\mathbf{A}$ by its idempotent reduct. From Fact 4.4, we know that $\mathbf{A}$ is simple and there exists a cyclic subuniverse R of $\mathbf{A}^p$ with no constant tuple. The minimality of $\mathbf{A}$ implies that R is subdirect, and since A can't have just one element, by Theorem 3.2, we obtain a retraction of the relational structure (A, R) onto a substructure (A', R') , where $|A'| < |A|$. Since, for some n , (A, R) is $\mathcal{J}_n$ -compatible, then, by Proposition 4.3, (A', R') is $\mathcal{J}_n$ -compatible as well. As (A', R') is a retraction of (A, R) and R is cyclic, R' is cyclic too. Using Fact 4.4 and the 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] Barto, L., Kozik, M., Maróti, M., McKenzie, R., Niven, T.: Congruence modularity implies cyclic terms for finite algebras (2007). *Algebra Universalis* **61**, 365–380 (2009)
- [2] Barto, L., Kozik, M., Niven, T.: 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] Hobby, D., McKenzie, R.: The structure of finite algebras, Contemporary Mathematics, vol. 76. American Mathematical Society, Providence, RI (1988)
- [4] Kearnes, K.A.: Congruence join semidistributivity is equivalent to a congruence identity. *Algebra Universalis* **46**(3), 373–387 (2001)
- [5] Maróti, M., McKenzie, R.: Existence theorems for weakly symmetric operations. *Algebra Universalis* **59**(3-4), 463–489 (2008)

LIBOR BARTO

Department of Algebra, Charles University, Prague, Czech Republic
e-mail: barto@karlin.mff.cuni.cz

MARCIN KOZIK

Department of Theoretical Computer Science, Jagiellonian University, Kraków, Poland
e-mail: Marcin.Kozik@tcs.uj.edu.pl

Open Access This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.