Algebra Univers. 61 (2009) 365–380
DOI 10.1007/s00012-009-0025-z
Published online October 30, 2009

Algebra Universalis

Congruence modularity implies cyclic terms for finite algebras

Libor Barto, Marcin Kozik, Miklós Maróti, Ralph McKenzie, and Todd Niven

Abstract. An n-ary operation $f\colon A^n \to A$ is called cyclic if it is idempotent and $f(a_1, a_2, a_3, \dots, a_n) = f(a_2, a_3, \dots, a_n, a_1)$ for every $a_1, \dots, a_n \in A$. We prove that every finite algebra $\mathbf{A}$ in a congruence modular variety has a p-ary cyclic term operation for any prime p greater than $|A|$.

1. Introduction

One motivation of the work described in this paper is the constraint satisfaction problem, which asks, for a fixed relational structure $\mathbb{B}$, the computational complexity of deciding whether a similar structure $\mathbb{A}$ can be mapped homomorphically to $\mathbb{B}$. The dichotomy conjecture of Feder and Vardi [6] states that for any $\mathbb{B}$ this problem is either NP-complete or solvable in polynomial time. Bulatov, Krokhin and Jeavons in [3] have shown that the computational complexity of the constraint satisfaction problem depends only on the clone of polymorphisms of $\mathbb{B}$, and were able to reformulate the dichotomy conjecture in the language of finite idempotent algebras. They conjecture that if all relations of $\mathbb{B}$ are subpowers of an algebra $\mathbf{B}$ on the same universe and $\mathbf{B}$ satisfies a nontrivial idempotent Maltsev condition, then the constraint satisfaction problem for $\mathbb{B}$ is solvable in polynomial time.

Families of locally finite varieties satisfying certain congruence conditions (e.g., congruence distributivity, permutability, or modularity) have various well known characterizations by nontrivial idempotent Maltsev conditions and by omitting certain types of congruence covers as defined in the tame congruence theory [9] of Hobby and McKenzie. From tame congruence theory we have a fairly good understanding of the polynomials of finite algebras and their relation to congruence covers, which has been applied very successfully in

Presented by E. Kiss.

Received November 30, 2007; accepted in final form February 26, 2008.

2000 *Mathematics Subject Classification*: Primary: 08B10; Secondary: 08B05.

Key words and phrases: Maltsev condition, cyclic term, congruence modularity, weak near-unanimity.

The first author was supported by the Grant Agency of the Czech Republic under grant no. 201/06/0664 and by the project of Ministry of Education under grant no. MSM 0021620839. The second and fifth authors were supported by the Eduard Čech Center grant LC505. The third author was partially supported by the Hungarian National Foundation for Scientific Research (OTKA), grant nos. T 48809 and K 60148. The fourth author was supported by the US National Science Foundation, grant no. DMS 0604065.

several settings. However, for the proof of the dichotomy conjecture, it seems, we need a better understanding of term operations. If **B** has a near-unanimity term, then we know that the corresponding constraint satisfaction problem is solvable in polynomial time using the notion of "bounded relational width," see [6]. But even for algebras in a congruence distributive variety the conjecture of Bulatov, Krokhin and Jeavons is still open; however there are partial results [5, 10].

Maróti and McKenzie in [13] have shown that any locally finite variety satisfying a nontrivial idempotent Maltsev condition has a term t of arity at least two that satisfies the identities

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

which is called a *weak near-unanimity* term. Congruence meet-semidistributive locally finite varieties have also been characterized in terms of weak near-unanimity term operations. It is still not fully understood how weak near-unanimity terms could be applied in the study of the constraint satisfaction problem. However, there might exist even "stronger" terms in these Maltsev classes which could be directly applicable, such as the cyclic terms studied in this paper.

A term t of arity at least two is *cyclic* if it satisfies the identities

$$t(x, x, \dots, x) \approx x,$$
$$t(x_1, x_2, x_3, \dots, x_n) \approx t(x_2, x_3, \dots, x_n, x_1).$$

Clearly, every cyclic term is a weak near-unanimity term. The chief result of this paper is the proof that for any finite algebra **A** in a congruence modular variety and a prime integer p greater than $|A|$, there exists a p-ary cyclic term of **A**. However, the following example shows that we cannot avoid the assumption $p > |A|$, and we cannot generalize this result to locally finite varieties.

Consider the algebra $\mathbf{A} = (A; f)$, where f is the ternary discriminator, that is,

$$f(a, b, c) = \begin{cases} a & \text{if } a \neq b, \\ c & \text{if } a = b. \end{cases}$$

The term operations of this algebra are just the conservative pattern operations. This means that for any term t of arity $n \leq |A|$, there is a fixed index i with $1 \leq i \leq n$ so that we have $t(a_1, \dots, a_n) = a_i$ whenever the elements $a_1, \dots, a_n \in A$ are pairwise distinct. Therefore t cannot be cyclic and **A** has no cyclic term of arity less than or equal to $|A|$. On the other hand, discriminator varieties are arithmetical (both congruence distributive and permutable), so if A is finite, then **A** has p-ary cyclic terms for any prime $p > |A|$ by the main result of this paper. Now consider the variety $\mathcal{V}$ generated by $\mathbf{N} = (N; f)$ where N is the set of natural numbers. By the previous argument $\mathcal{V}$ has no cyclic term and $\mathcal{V}$ is arithmetical. Observe that all permutations of N are automorphisms of $\mathbf{N}$, and any subset of N is a subuniverse of $\mathbf{N}$. Therefore, for any two n-ary terms s, t, $\mathcal{V} \models s \approx t$ if and only if $(\{1, \dots, n\}; f) \models s \approx t$. Hence $\mathcal{V}$ is locally finite.

The following questions naturally arise.

Question 1.1. Let $\mathbf{A}$ be a finite algebra in a variety omitting types **1** and **2**, or, more generally, omitting type **1**. What can be said about cyclic terms of $\mathbf{A}$? In particular

(1) Does $\mathbf{A}$ have a cyclic term?
(2) Does $\mathbf{A}$ have a cyclic term of arity p for almost all primes?
(3) Does $\mathbf{A}$ have a cyclic term of arity p for all primes $p > |A|$?

2. Cyclic terms

The semantic meaning of the existence of a cyclic term is shown in the following proposition.

Proposition 2.1. *Let $\mathcal{V}$ be a variety. The following are equivalent:*

(1) *$\mathcal{V}$ has an n-ary cyclic term.*
(2) *For all $\mathbf{A} \in \mathcal{V}$ and $\alpha \in \operatorname{Aut}(\mathbf{A})$, if $\alpha^n = \mathrm{id}_A$, then α has a fixed point.*

Proof. Assume that $\mathcal{V}$ has an n-ary cyclic term t, that $\mathbf{A} \in \mathcal{V}$ and $\alpha \in \operatorname{Aut}(\mathbf{A})$ so that $\alpha^n = \mathrm{id}_A$. Then for any $a \in A$,

$$\begin{aligned}\alpha(t(a, \alpha(a), \dots, \alpha^{n-1}(a))) &= t(\alpha(a), \alpha^2(a), \dots, \alpha^{n-1}(a), \alpha^n(a))\\ &= t(\alpha(a), \alpha^2(a), \dots, \alpha^{n-1}(a), a)\\ &= t(a, \alpha(a), \dots, \alpha^{n-1}(a));\end{aligned}$$

thus the element $t(a, \alpha(a), \dots, \alpha^{n-1}(a))$ is a fixed point of α.

On the other hand, let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(n)$ and let $\alpha \in \operatorname{Aut}(\mathbf{F})$ be generated by its action on the free generators: $\alpha(x_i) = x_{i+1 \bmod n}$. Clearly, $\alpha^n = \mathrm{id}_F$, so let $t \in \mathbf{F}$ be a fixed point of α. Then $t(x_1, \dots, x_n) = (\alpha(t))(x_1, \dots, x_n) = t(x_2, \dots, x_n, x_1)$ in $\mathbf{F}$, which is equivalent to the identity $\mathcal{V} \models t(x_1, \dots, x_n) \approx t(x_2, \dots, x_n, x_1)$. □

Proposition 2.2. *For an algebra $\mathbf{A}$, let*

$$C(\mathbf{A}) = \{n \in \omega \mid n \geq 2 \textit{ and } \mathbf{A} \textit{ has an } n\textit{-ary cyclic term}\}.$$

The following two properties hold for $C(\mathbf{A})$:

(1) *If $n \in C(\mathbf{A})$ and $1 < k \mid n$, then $k \in C(\mathbf{A})$.*
(2) *If $m, n \in C(\mathbf{A})$, then $mn \in C(\mathbf{A})$. In particular, all powers of n are in $C(\mathbf{A})$.*

Therefore, $C(\mathbf{A})$ is completely determined by the set of primes in $C(\mathbf{A})$ and is equal to all products of powers of those primes.

Proof. For the first statement, assume that the term $t(x_1, x_2, \dots, x_n)$ is cyclic, and take

$$t_1(x_1, \dots, x_k) = t(\underbrace{x_1, \dots, x_k, x_1, \dots, x_k, \dots, x_1, \dots, x_k}_{n/k \text{ times}}).$$

Clearly, t_1 is a cyclic term since t is.

For the second statement, let $t_1(x_1, x_2, \dots, x_m)$ and $t_2(x_1, x_2, \dots, x_n)$ be cyclic, and put

$$\begin{aligned} t(x_1, x_2, \dots, x_{mn}) = t_1\bigl(&t_2(x_1, x_{m+1}, \dots, x_{m(n-1)+1}),\\ &t_2(x_2, x_{m+2}, \dots, x_{m(n-1)+2}), \dots, t_2(x_m, x_{2m}, \dots, x_{mn})\bigr). \end{aligned}$$

Then

$$\begin{aligned} t(x_2, \dots, x_{mn}, x_1) &= t_1\bigl(t_2(x_2, x_{m+2}, \dots, x_{m(n-1)+2}), \dots,\\ &\qquad t_2(x_n, x_{2m}, \dots, x_{mn}), t_2(x_{m+1}, \dots, x_{m(n-1)+1}, x_1)\bigr)\\ &= t_1\bigl(t_2(x_2, x_{m+2}, \dots, x_{m(n-1)+2}), \dots,\\ &\qquad t_2(x_n, x_{2m}, \dots, x_{mn}), t_2(x_1, x_{m+1}, \dots, x_{m(n-1)+1})\bigr)\\ &= t_1\bigl(t_2(x_1, x_{m+1}, \dots, x_{m(n-1)+1}), t_2(x_2, x_{m+2}, \dots, x_{m(n-1)+2}), \dots,\\ &\qquad t_2(x_n, x_{2m}, \dots, x_{mn})\bigr) = t(x_1, x_2, \dots, x_{mn}) \end{aligned}$$

(the second equality follows from the fact that t_2 is cyclic, while the third one follows from the fact that t_1 is cyclic). □

Definition 2.3. For an algebra $\mathbf{A}$ and an integer n, define $\sigma\colon A^n \to A^n$ as

$$\sigma\colon (a_1, a_2, \dots, a_n) \mapsto (a_2, \dots, a_n, a_1).$$

By a *cyclically symmetric subuniverse* of $\mathbf{A}^n$ we mean a subuniverse of $\mathbf{A}^n$ that is closed under σ. Clearly, this notion defines a closure operator, and we can talk about the cyclically symmetric subuniverse generated by a tuple $\bar{a} \in A^n$.

Lemma 2.4. *Let $\mathbf{A}$ be a finite idempotent algebra and $n \geq 2$ be a natural number. The following are equivalent:*

(1) *$\mathbf{A}$ has an n-ary cyclic term operation.*
(2) *There exists an n-ary term operation $t \in \mathrm{Clo}_n(\mathbf{A})$ such that, for any $\bar{a} \in A^n$, $t(\bar{a}, \sigma(\bar{a}), \dots, \sigma^{n-1}(\bar{a}))$ is a constant tuple.*
(3) *For any $\bar{a} \in A^n$ there is an n-ary term operation $t \in \mathrm{Clo}_n(\mathbf{A})$ such that $t(\bar{a}, \sigma(\bar{a}), \dots, \sigma^{n-1}(\bar{a}))$ is a constant tuple.*
(4) *For any $\bar{a} \in A^n$, the cyclically symmetric subuniverse generated by $\bar{a}$ contains a constant tuple.*

Proof. (1) ⇒ (2) is obvious: take t to be an n-ary cyclic term. (2) ⇐ (1) is immediate as well: a term t satisfying the condition (2) is cyclic. (2) ⇒ (3) is trivial.

Let us prove (3) $\Rightarrow$ (2). For a term $t \in \mathrm{Clo}_n(\mathbf{A})$ we define $S(t) \subseteq A^n$ to be the set of all $\bar{a} \in A^n$ such that $t(\bar{a}) = t(\sigma(\bar{a})) = \cdots = t(\sigma^{n-1}(\bar{a}))$. Let t be such that $|S(t)|$ is maximal. We claim that t satisfies the condition (2) and assume that it does not, that is, there exists a tuple $\bar{a} \in A^n$ such that $t(\bar{a}) = t(\sigma(\bar{a})) = \cdots = t(\sigma^{n-1}(\bar{a}))$ fails. Consider the tuple $\bar{b} \in A^n$ defined by $b_i = t(\sigma^i(\bar{a}))$, $1 \leq i \leq n$. According to our assumptions, there exists a term $t_{\bar{b}} \in \mathrm{Clo}_n(\mathbf{A})$ such that $\bar{b} \in S(t_{\bar{b}})$. Now consider the term

$$s = t_{\bar{b}}(t(x_1, \dots, x_n), t(x_2, \dots, x_n, x_1), \dots, t(x_n, x_1, \dots, x_{n-1})).$$

We claim that $S(t) \subseteq S(s)$, but also that $\bar{a} \in S(s)$. This would clearly be a contradiction with the maximality of $|S(t)|$.

Let $\bar{x} \in S(t)$. Then $s(\sigma^i(\bar{x})) = t_{\bar{b}}(t(\sigma^i(\bar{x})), t(\sigma^{i+1}(\bar{x})), \dots, t(\sigma^{i-1}(\bar{x}))) = t_{\bar{b}}(t(\bar{x}), t(\bar{x}), \dots, t(\bar{x})) = t(\bar{x})$ for all i, so $\bar{x} \in S(s)$. On the other hand, $s(\sigma^i(\bar{a})) = t_{\bar{b}}(t(\sigma^i(\bar{a})), t(\sigma^{i+1}(\bar{a})), \dots, t(\sigma^{i-1}(\bar{a}))) = t_{\bar{b}}(b_i, b_{i+1}, \dots, b_{i-1}) = t_{\bar{b}}(\sigma^i(\bar{b}))$, which is constant for all i by the choice of $t_{\bar{b}}$. Therefore $\bar{a} \in S(s)$ and the contradiction is established.

(2) $\Rightarrow$ (4) is trivial. To prove (4) $\Rightarrow$ (3) observe that the fact that a constant tuple $\bar{b} = (b, b, \dots, b)$ is in the subalgebra generated by $\{\bar{a}, \sigma(\bar{a}), \dots, \sigma^{n-1}(\bar{a})\}$ means that there exists a term t such that $t(\bar{a}, \sigma(\bar{a}), \dots, \sigma^{n-1}(\bar{a})) = \bar{b}$, which implies that $t(\bar{a}) = t(\sigma(\bar{a})) = \cdots = t(\sigma^{n-1}(\bar{a}))$. □

Lemma 2.5. *Let* $\mathbf{A}$ *be a finite idempotent algebra with no cyclic term of arity* p*, and suppose that* $\mathbf{A}$ *is of minimal cardinality with this property in the variety generated by* $\mathbf{A}$*. Then* $\mathbf{A}$ *is simple.*

Proof. Suppose that $\mathbf{A}$ is not simple, and θ is a congruence of $\mathbf{A}$, $0_A < \theta < 1_A$. According to Lemma 2.4, to get a contradiction, we only need to show that every cyclically symmetric subalgebra $\mathbf{S}$ of $\mathbf{A}^p$ contains a diagonal element. Let $\pi\colon \mathbf{A} \to \mathbf{A}/\theta$ be the canonical map. Then $\{\, \pi(\bar{x}) : \bar{x} \in S \,\}$ is a non-void cyclically symmetric subuniverse of $(\mathbf{A}/\theta)^p$. By our minimality assumption, it follows that there is $\bar{x} \in S$ such that $\{x_i : 0 \leq i < p\}$ is contained in one θ-equivalence class Q. Since $\mathbf{A}$ is idempotent, Q is a subuniverse and we have the algebra $\mathbf{Q}$. Now $Q^p \cap S$ is a non-void cyclically symmetric subuniverse of $\mathbf{Q}^p$. Again by minimality of $\mathbf{A}$, there is a diagonal element $(a, \dots, a)$ in $Q^p \cap S$. This is a contradiction, and it shows that $\mathbf{A}$ is simple. □

3. Nicely connected graphs

By a (directed) graph $\mathbb{G} = (A, E)$ we mean an arbitrary binary relation $E \subseteq A^2$ on a non-empty set A. All graphs in this paper are directed. We sometimes write $x \xrightarrow{\mathbb{G}} y$ to denote $(x, y) \in E$, or just $x \to y$, if there is no danger of confusion.

A *path* of length n ($n \geq 0$) in a graph $\mathbb{G} = (A, E)$ is a sequence $a_0, \dots, a_n \in A$ of elements such that $(a_i, a_{i+1}) \in E$ for all $i < n$. We write $x \xrightarrow{n,\mathbb{G}} y$ to denote that there is a path of length n in $\mathbb{G}$ from x to y. A path $a_0, \dots, a_n$

is called a *cycle* if $a_0 = a_n$; so a cycle can intersect itself. A *loop* is a cycle of length 1. A graph is *trivial* if it has a single element and no edge. A graph is *strongly connected* if for any pair a, b of its elements there is a path from a to b. In particular, the trivial graph is strongly connected, and every other strongly connected graph has at least one edge. A *strong component* of $\mathbb{G}$ is a maximal (under inclusion) strongly connected induced subgraph of $\mathbb{G}$.

For a graph $\mathbb{G} = (A, E)$, a subset $B \subseteq A$ and an integer $k \geq 0$ we define

$$\mathcal{N}_{\mathbb{G}}(B, k) = \{\, a \in A : \exists\, b \in B \; b \xrightarrow{k,\mathbb{G}} a \,\},$$
$$\mathcal{N}_{\mathbb{G}}(B, -k) = \{\, a \in A : \exists\, b \in B \; a \xrightarrow{k,\mathbb{G}} b \,\}.$$

For a finite graph $\mathbb{G}$ containing at least one cycle we define $\zeta(\mathbb{G})$ to be the greatest common divisor of the length of all cycles in $\mathbb{G}$. Without going into the details, we note that $\zeta(\mathbb{G})$ equals the algebraic length of the graph $\mathbb{G}$, if $\mathbb{G}$ is strongly connected (see [1]). A graph $\mathbb{G} = (A, E)$ is *nicely connected* if it is strongly connected, $E \neq \emptyset$, and $\zeta(\mathbb{G}) = 1$.

Lemma 3.1. *Let $\mathbb{G} = (A, E)$ be a finite, nontrivial, strongly connected graph.*

(1) *For any $a, b \in A$, if p and q are any two paths in $\mathbb{G}$ from a to b then their lengths are congruent modulo $\zeta(\mathbb{G})$.*
(2) *If $\zeta(\mathbb{G}) = 1$, then there is an integer $K > 0$ such that for any $k \geq K$ and $a, b \in A$ there is a path of length k from a to b.*
(3) *There is an integer $K > 0$ such that for any $k \geq K$ and $a, b \in A$ there is a path from a to b of length $k \cdot \zeta(\mathbb{G}) + i$ for some $0 \leq i < \zeta(\mathbb{G})$.*
(4) *If $\zeta(\mathbb{G}) = 1$ and $a \in A$, then $\mathcal{N}_{\mathbb{G}}(\{a\}, k) = A$ for some integer $k > 0$.*

Proof. To prove (1) take a path r from b to a, so we have two cycles p, r and q, r, and the length of both are divisible by $\zeta(\mathbb{G})$, thus the claim follows.

To show (2), take cycles $p_1, \dots, p_t$ in $\mathbb{G}$ of length $\ell_1, \dots, \ell_t$ such that $\zeta(\mathbb{G}) = \gcd(\ell_1, \dots, \ell_t)$. It is well known that there is a natural number M such that every $m \geq M$ can be written as a sum of elements from $\{\ell_1, \ell_1, \dots, \ell_t\}$. (For a lower bound on this number, due to Schur, see [2].) For any $a, b \in A$, there is a path from a to b of length no greater than $(t+1)|G|$ that goes through some vertex of each cycle in $p_1, \dots, p_t$. Concatenating this path with the required cycles in $p_1, \dots, p_t$ (where they intersect) the required number of times, we get for any $k \geq M + (t+1)|G|$ a path of length k from a to b.

Statement (3) is just a slight generalization of (2) and can be proved similarly, while (4) is an immediate consequence of (2). □

Definition 3.2. By a graph over an algebra $\mathbf{A}$ we mean a graph (A, E) with vertex-set A and edge-set E a subuniverse of $\mathbf{A}^2$.

Lemma 3.3. *Let $\mathbb{G} = (A, E)$ be a graph over an idempotent algebra $\mathbf{A}$.*

(1) *For any subuniverse U of $\mathbf{A}$ and integer k, $\mathcal{N}_{\mathbb{G}}(U, k)$ is a subuniverse of $\mathbf{A}$. In particular, $\mathcal{N}_{\mathbb{G}}(\{a\}, k)$ is a subuniverse of $\mathbf{A}$ for any $a \in A$.*

(2) *If $\mathbb{H} = (H, E \cap H^2)$ is a nontrivial strong component of $\mathbb{G}$ and $\zeta(\mathbb{H}) = 1$, then H is a subuniverse of $\mathbf{A}$.*

Proof. First we prove the statement (1) for $k = 1$. Let U be a subuniverse of $\mathbf{A}$, and put $V = \mathcal{N}_{\mathbb{G}}(U, 1)$. Take an n-ary operation t of $\mathbf{A}$, and elements $v_1, \dots, v_n \in V$. By the definition of $\mathcal{N}_{\mathbb{G}}(U, 1)$, there exist elements $u_1, \dots, u_n \in U$ so that $u_1 \to v_1, \dots, u_n \to v_n$. Since E is a subuniverse of $\mathbf{A}^2$,

$$t(u_1, \dots, u_n) \to t(v_1, \dots, v_n).$$

But U is a subuniverse of $\mathbf{A}$, so $t(u_1, \dots, u_n) \in U$, and thus $t(v_1, \dots, v_n) \in V$. This proves that V is a subuniverse of $\mathbf{A}$. The proof of the $k = -1$ case is analogous, and then the general case follows as $\mathcal{N}_{\mathbb{G}}(U, k+1) = \mathcal{N}_{\mathbb{G}}(\mathcal{N}_{\mathbb{G}}(U, k), 1)$ for $k \geq 0$, and $\mathcal{N}_{\mathbb{G}}(U, k-1) = \mathcal{N}_{\mathbb{G}}(\mathcal{N}_{\mathbb{G}}(U, k), -1)$ for $k \leq 0$.

To prove statement (2), note that $\mathbb{H}$ is nicely connected. From Lemma 3.1 there exists an integer k so that $H = \mathcal{N}_{\mathbb{H}}(\{a\}, k) \cap \mathcal{N}_{\mathbb{H}}(\{a\}, -k)$ for some element $a \in H$. Thus $H \subseteq \mathcal{N}_{\mathbb{G}}(\{a\}, k) \cap \mathcal{N}_{\mathbb{G}}(\{a\}, -k)$. But the right hand side is strongly connected (every element is in a cycle of length $2k$ that goes through a), and H is a maximal strongly connected induced subgraph, so $H = \mathcal{N}_{\mathbb{G}}(\{a\}, k) \cap \mathcal{N}_{\mathbb{G}}(\{a\}, -k)$. This proves that H is a subuniverse by statement (1). □

Theorem 3.4. *Let $\mathbf{A}$ be a finite algebra possessing a cyclic term of arity at least 2. Then every nicely connected graph $\mathbb{G}$ over $\mathbf{A}$ has a loop.*

Proof. By Proposition 2.2 we may assume that $\mathbf{A}$ has a cyclic term of arity p for some prime p. Let $\mathbb{G} = (A, E)$ be a nicely connected graph over $\mathbf{A}$. By Lemma 3.1, there exists an integer K such that for any $k \geq K$ and elements $a, b \in A$ there exists a path from a to b of length k. Choose k to be larger than K and to be a power of p. Then, by Proposition 2.2, there exists a cyclic term t of arity k, and a cycle $a_0, \dots, a_k = a_0$ of length k in $\mathbb{G}$. Since E is a subalgebra of $\mathbf{A}^2$, and $a_i \to a_{i+1}$ for all $0 \leq i < k$, the pair $(t(a_0, \dots, a_{k-1}), t(a_1, \dots, a_k))$ is an edge of $\mathbb{G}$. But t is cyclic, so $t(a_0, \dots, a_{k-1}) = t(a_1, \dots, a_{k-1}, a_0) = t(a_1, \dots, a_k)$. Consequently, this edge is a loop. □

4. Congruence distributivity

First we show a restricted version of the converse of Theorem 3.4 for finite algebras in a congruence join-semidistributive variety. An algebra $\mathbf{A}$ is congruence join-semidistributive if whenever α, β, γ are congruences of $\mathbf{A}$ with $\alpha \vee \beta = \alpha \vee \gamma$, then $\alpha \vee \beta = \alpha \vee (\beta \wedge \gamma)$. Clearly, distributivity implies join-semidistributivity. Other than in the following lemma we will not work with congruence join-semidistributivity.

Lemma 4.1. *Let p be a prime, let $\mathbf{A}$ be a finite idempotent algebra with no cyclic term of arity p, and suppose that $\mathbf{A}$ is of minimal cardinality with this* *property in the variety generated by* $\mathbf{A}$ *and that* $p > |A|$*. Assume that every finite subdirect power of* $\mathbf{A}$ *is congruence join-semidistributive. Then*

(1) *there exists a nicely connected graph* $\mathbb{G} = (G, E)$ *without loops on a subdirect power* $\mathbf{G}$ *of* $\mathbf{A}$*, such that*

(2) *for any proper subuniverse* H *of* $\mathbf{G}$*, the induced graph* $\mathbb{H} = (H, E \cap H^2)$ *is not nicely connected.*

Proof. By Lemma 2.5, $\mathbf{A}$ is simple. Let $\mathbf{S}$ be a minimal non-void cyclically symmetric subalgebra of $\mathbf{A}^p$ that has no diagonal element. By the minimality of $\mathbf{A}$, $\mathbf{S}$ is a subdirect power of $\mathbf{A}$, and by minimality of S, for all $(a_1, \dots, a_p) \in S$ we have that $\{a_1, \dots, a_p\}$ generates $\mathbf{A}$.

We define a graph $\mathbb{V} = (V, E)$ over a subalgebra $\mathbf{V}$ of $\mathbf{A}^{p-1}$ that will be held fixed for the remainder of the proof. V is the set of all $(x_1, \dots, x_{p-1}) \in A^{p-1}$ such that $(x_1, \dots, x_{p-1}, x) \in S$ for some $x \in A$. E is the set of all pairs $(\bar{x}, \bar{y}) \in V^2$ such that for some $(a_1, \dots, a_p) \in S$, $\bar{x} = (a_1, \dots, a_{p-1})$ and $\bar{y} = (a_2, \dots, a_p)$.

Obviously, V is a subuniverse of $\mathbf{A}^{p-1}$ and E is a subuniverse of $\mathbf{A}^{2p-2}$. So $\mathbb{V}$ is a graph over $\mathbf{V}$. We claim that $\mathbb{V}$ is nicely connected and has no loops. First, if $(\bar{x}, \bar{y}) \in E$ with $\bar{x} = \bar{y}$, then we have $\bar{a} = (a_1, \dots, a_p) \in S$ with $a_i = x_i = y_i = a_{i+1}$ for all $1 \leq i < p$, i.e., $\bar{a}$ is a diagonal element, which is a contradiction. Thus $\mathbb{V}$ has no loops.

To see that $\mathbb{V}$ is strongly connected, define η_i to be the ith projection congruence on $\mathbf{S}$, $1 \leq i \leq p$, and define $\eta'_i = \bigwedge_{j \neq i} \eta_j$. We have two cases: either $\eta_i \vee \eta_j = 1_S$ for $i \neq j$, or else $\eta_i = \eta_j$ for some $i \neq j$, since $\mathbf{A} \cong \mathbf{S}/\eta_i$ is simple. If $\eta_i = \eta_j$ for some $i \neq j$, then by the cyclic symmetry of S and the primality of p we have $\eta_1 = \eta_2 = \cdots = \eta_p$ and since $\bigwedge \eta_i = 0_S$, then $\eta_i = 0_S$ for all i. Take a tuple $\bar{a} \in S$. Since $p > |A|$, two coordinates of $\bar{a}$ must be equal, say $a_i = a_j$ for some $i < j$, and therefore $(\sigma^{j-i}(\bar{a}), \bar{a}) \in \eta_i = 0_S$. This implies that $a_{(i+k \bmod p)+1} = a_{(j+k \bmod p)+1}$ for all k; therefore $\bar{a}$ is a diagonal element of $\mathbf{S}$, which is a contradiction.

So we have $\eta_i \vee \eta_j = 1_S$ for $i \neq j$. Since the congruence lattice of $\mathbf{S}$ is join-semidistributive, it follows easily that $\eta_i \vee \eta'_i = 1_S$, and then $\eta_j \vee (\bigvee_i \eta'_i) = 1_S$ for all j, so $(\bigwedge_j \eta_j) \vee (\bigvee_i \eta'_i) = 1_S$ and $\bigvee_i \eta'_i = 1_S$.

If $(\bar{a}, \bar{b}) \in \eta'_i$, then

$$\begin{aligned}(a_1, \dots, a_{p-1}) \to (a_2, \dots, a_p) \to \cdots \to (a_{i+1}, \dots, a_{i-1}) = \\ (b_{i+1}, \dots, b_{i-1}) \to (b_{i+2}, \dots, b_i) \to \cdots \to (b_1, \dots, b_{p-1})\end{aligned}$$

is a path of length p in the graph $\mathbb{V}$. As $\bigvee_i \eta'_i = 1_S$, this easily implies that $\mathbb{V}$ is strongly connected. Moreover, we also get that every member of V belongs to a p-cycle, and in fact any two members of V can be connected by a path whose length is a multiple of p. In particular, there is a path of length kp connecting $(a_2, \dots, a_p)$ to $(a_1, \dots, a_{p-1})$ for some integer k, which gives a cycle of length $kp+1$ for $(a_2, \dots, a_p)$. Thus it follows that $\zeta(\mathbb{V})$, a divisor of both p and $kp+1$, is 1. So $\mathbb{V}$ is nicely connected.

Let G be a subuniverse of $\mathbf{V}$ of minimal cardinality such that the induced graph $\mathbb{G} = (G, E \cap G^2)$ is nicely connected. To finish the proof we need to show that G is a subdirect power of $\mathbf{A}$. Take a cycle $\bar{x}^1, \ldots, \bar{x}^{m-1} = \bar{x}^1$ in $\mathbb{G}$ of length m (with $m > 1$ of course), where we can assume, by concatenating a cycle with itself many times, that $m > p$. Now there is $\bar{a} \in S$ such that $(a_1, \ldots, a_{p-1}) = \bar{x}^1$ and $(a_2, \ldots, a_p) = \bar{x}^2$. Thus $x_1^i = a_i$ for all $1 \leq i \leq p$. From the minimality of S we already know that $a_1, \ldots, a_p$ generate $\mathbf{A}$. Thus $\{z_1 : \bar{z} \in G\}$ generates $\mathbf{A}$, and it follows that G projects onto A at the first coordinate. Also, if $\bar{x} \in G$ and $2 \leq i \leq p$, then there is a path in G, $\bar{y}^1, \ldots, \bar{y}^i = \bar{x}$ with $(\bar{y}^j, \bar{y}^{j+1}) \in E$ for $1 \leq j < i$. Here, $x_1 = y_i^1$. Thus also G projects onto A at the ith coordinate. □

If $\mathbf{A}$ is an algebra in a congruence distributive variety, then there exists a sequence $J_0, J_1, \ldots, J_{2m}$ of ternary terms satisfying the Jónsson equations [4]:

$$\begin{aligned} J_0(x,y,z) &\approx x, \\ J_{2k}(x,y,y) &\approx J_{2k+1}(x,y,y) && \text{for } 0 \leq k < m, \\ J_{2k+1}(x,x,y) &\approx J_{2k+2}(x,x,y) && \text{for } 0 \leq k < m, \\ J_{2m}(x,y,z) &\approx z, \\ J_i(x,y,x) &\approx x && \text{for all } 0 \leq i \leq 2m. \end{aligned}$$

Without loss of generality, we may assume that the basic operations of $\mathbf{A}$ are exactly the Jónsson operations $J_0, \ldots, J_{2m}$. Henceforth we work with algebras of this fixed signature and assume that they satisfy the Jónsson equations, and consequently they are idempotent.

Definition 4.2. By a *Jónsson ideal* in an algebra $\mathbf{A}$ we mean a subuniverse U of $\mathbf{A}$ such that whenever $0 \leq i \leq 2m$, $u, v \in U$ and $a \in A$ then $J_i(u, a, v) \in U$.

Clearly, the set of Jónsson ideals of $\mathbf{A}$ is closed under intersection.

Lemma 4.3. *Let $\mathbb{G} = (A, E)$ be a graph over an algebra $\mathbf{A} = (A; J_0, \ldots, J_{2m})$ with Jónsson operations.*

(1) *Every one-element subset $\{a\} \subseteq A$ is a Jónsson ideal of $\mathbf{A}$.*
(2) *If U is a Jónsson ideal of $\mathbf{A}$, and $A = \mathcal{N}_{\mathbb{G}}(A, 1)$, then $\mathcal{N}_{\mathbb{G}}(U, k)$ is also a Jónsson ideal for any integer k.*

Proof. Since $\mathbf{A}$ is idempotent and for all $0 \leq i \leq 2m$ it satisfies the identity $J_i(x, y, x) \approx x$, every one-element subset $\{a\} \subseteq A$ is a Jónsson ideal.

Note that it is enough to prove statement (2) for $k = 1$, just like in the proof of Lemma 3.3 (1). Put $V = \mathcal{N}_{\mathbb{G}}(U, 1)$ and take elements $a_1, c_1 \in V$ and $b_1 \in A$. By definition of V, there are elements $a_0, c_0 \in U$ so that $a_0 \to a_1$, $c_0 \to c_1$, and by the assumption $\mathcal{N}_{\mathbb{G}}(A, 1) = A$ there is $b_0 \in A$ so that $b_0 \to b_1$. Take any basic operation J_i. Then $J_i(a_0, b_0, c_0) \to J_i(a_1, b_1, c_1)$ as E is a subuniverse of $\mathbf{A}^2$. As U was a Jónsson ideal, $J_i(a_0, b_0, c_0) \in U$, and therefore $J_i(a_1, b_1, c_1) \in V$. This proves that V is a Jónnson ideal of $\mathbf{A}$. □

Theorem 4.4. *Let* $\mathbf{A}$ *be a finite algebra in a congruence distributive variety, and let* $\mathbb{G} = (A, E)$ *be a nicely connected graph over* $\mathbf{A}$*. Then* $\mathbb{G}$ *contains a loop.*

Proof. Suppose the opposite, and take a minimal counterexample with respect to $|A|$. Without loss of generality, we may assume that $\mathbf{A}$ has only the Jónsson terms $J_0, \dots, J_{2m}$ as basic operations, and therefore $\mathbf{A}$ is idempotent. Fix an element $g \in A$. By Lemma 3.1, there is an integer r such that $\mathcal{N}_{\mathbb{G}}(\{g\}, r) = A$. Suppose that r is minimal with respect to this property, thus $B = \mathcal{N}_{\mathbb{G}}(\{g\}, r-1)$ is a proper subset of A. From Lemma 4.3 we know that B is a Jónsson ideal of $\mathbf{A}$.

We claim that the induced graph $\mathbb{B} = (B, E \cap B^2)$ contains a cycle. The number r was chosen so that $\mathcal{N}_{\mathbb{G}}(B, 1) = A$. Start with any element $b_0 \in B$. Since $\mathcal{N}_{\mathbb{G}}(B, 1) = A$, there is $b_1 \in B$ such that $b_1 \to b_0$. Similarly, there exists $b_2 \in B$ such that $b_2 \to b_1$. After sufficiently many steps $b_i = b_j$ for some $j < i$ and we have a cycle $b_i, b_{i-1}, \dots, b_j$ in $\mathbb{B}$.

Fix a cycle $b_0, \dots, b_{q-1}, b_q = b_0$ in $\mathbb{B}$. Since $\mathbb{G}$ is nicely connected, there exist paths $b_1 = a_0, a_1, \dots, a_{kq} = b_0$ and $b_0 = c_0, c_1, \dots, c_{kq} = b_1$ in $\mathbb{G}$ for some large enough integer k. By concatenating the cycle $b_0, \dots, b_q$ with itself k-many times we get the cycles $b_0, \dots, b_{kq} = b_0$ and $b_1, b_2, \dots, b_{kq}, b_{kq+1} = b_1$. For odd $0 < i < 2m$ let p_i be the path

$$\begin{aligned} J_i(b_0, b_1, b_1) = J_i(b_0, a_0, b_1) \to J_i(b_1, a_1, b_2) \to \cdots \\ \cdots \to J_i(b_{kq}, a_{kq}, b_{kq+1}) = J_i(b_0, b_0, b_1), \end{aligned}$$

and for even $0 < i < 2m$ let p_i be the path

$$\begin{aligned} J_i(b_0, b_0, b_1) = J_i(b_0, c_0, b_1) \to J_i(b_1, c_1, b_2) \to \cdots \\ \cdots \to J_i(b_{kq}, c_{kq}, b_{kq+1}) = J_i(b_0, b_1, b_1). \end{aligned}$$

The concatenation of the paths $p_1, \dots, p_{2m-1}$ gives the path

$$\begin{aligned} b_0 &= J_0(b_0, b_1, b_1) \\ &= J_1(b_0, b_1, b_1) \to \cdots \to J_1(b_0, b_0, b_1) \\ &= J_2(b_0, b_0, b_1) \to \cdots \to J_2(b_0, b_1, b_1) \\ &\vdots \\ &= J_{2m-1}(b_0, b_1, b_1) \to \cdots \to J_{2m-1}(b_0, b_0, b_1) \\ &= J_{2m}(b_0, b_0, b_1) = b_1 \end{aligned}$$

from b_0 to b_1 of length $(2m-1)kq$. Since the elements $b_0, \dots, b_{kq+1}$ are in B and B is a Jónsson ideal of $\mathbf{A}$, this path is in $\mathbb{B}$. However, $b_1, b_2, \dots, b_{q-1}, b_0$ is a path of length $q-1$ in $\mathbb{B}$, so we have a cycle of length $(2m-1)kq + q - 1$ in $\mathbb{B}$ containing b_0. Let C be the strong component of $\mathbb{B}$ containing b_0, and $\mathbb{C} = (C, E \cap C^2)$ be the induced subgraph. Then $\mathbb{C}$ contains the cycle constructed above of length $(2m-1)kq + q - 1$, and the cycle $b_0, \dots, b_q = b_0$ of length

q. This proves that $\zeta(\mathbb{C})$ is a divisor of $\gcd((2m-1)kq+q-1,q)=1$, and therefore $\mathbb{C}$ is nicely connected.

From Lemma 3.3 we get that C is a subuniverse of $\mathbf{A}$. Thus $\mathbb{C}$ is a nicely connected graph over the algebra $\mathbf{C}$ of size strictly smaller than $|A|$. This contradicts the minimality of $\mathbf{A}$. □

As a corollary of Lemma 4.1 (1) and Theorem 4.4 we get:

Theorem 4.5. *If* $\mathbf{A}$ *is a finite algebra in a congruence distributive variety, then for every prime* p *greater than* $|A|$*,* $\mathbf{A}$ *possesses a cyclic term of arity* p*.*

5. Congruence modularity

In this section we give a positive answer to Question 1.1 for algebras in a congruence modular variety. We start with a special case, congruence permutability.

Theorem 5.1. *Let* $\mathbf{A}$ *be a finite algebra with a Maltsev term. For every prime integer* p *greater than* $|A|$*,* $\mathbf{A}$ *possesses a cyclic term of* p *variables.*

Proof. Let p be a prime greater than $|A|$. According to Lemma 2.4, it is necessary and sufficient to show that every non-empty subuniverse S of $\mathbf{A}^p$ closed under the automorphism

$$\sigma\colon (x_1,\dots,x_p)\mapsto(x_2,\dots,x_p,x_1)$$

contains a diagonal element $(a,a,\dots,a)$.

Let us assume that this is false, and let $\mathbf{A}$ be a finite algebra of least cardinality for which it is false. We may assume that $\mathbf{A}$ has a single basic operation Q, which is a Maltsev term for $\mathbf{A}$. Thus $\mathbf{A}$ is idempotent with no cyclic term of arity p, and S is a non-void cyclically symmetric subuniverse of $\mathbf{A}^p$ containing no diagonal element. By Lemma 2.5, $\mathbf{A}$ is simple.

Note that the projection maps on S all map onto the same subuniverse D of $\mathbf{A}$. By minimality, $D=A$. Thus $\mathbf{S}$ is a subdirect power of $\mathbf{A}$. By Fleischer's Lemma (Corollary 10.2 in [4]), $\mathbf{S}\cong\mathbf{A}^k$ for some k, $1\le k\le p$. Thus p does not divide $|S|$.

Since $\sigma^p=\mathrm{id}$ on S, every orbit of σ on S has either 1 or p elements. Since p does not divide $|S|$, it follows that there is a one-element orbit. So there is $(x_1,\dots,x_p)\in S$ such that

$$(x_1,\dots,x_p)=(x_2,\dots,x_p,x_1).$$

Clearly, this is a diagonal element in S. This contradiction proves the theorem. □

If $\mathbf{A}$ is an algebra in a congruence modular variety, there exists a sequence $J_0, J_1, \dots, J_{2m}, Q$ of ternary terms satisfying the Gumm equations [8]:

$$\begin{aligned}
J_0(x,y,z) &\approx x, \\
J_{2k}(x,y,y) &\approx J_{2k+1}(x,y,y) && \text{for } 0 \le k < m, \\
J_{2k+1}(x,x,y) &\approx J_{2k+2}(x,x,y) && \text{for } 0 \le k < m, \\
J_{2m}(x,y,y) &\approx Q(x,y,y), \\
Q(x,x,y) &\approx y, \\
J_i(x,y,x) &\approx x && \text{for all } 0 \le i \le 2m.
\end{aligned}$$

Without loss of generality, we may assume that the basic operations of $\mathbf{A}$ are exactly the Gumm operations $J_0, \dots, J_{2m}, Q$. Henceforth we work with algebras of this fixed signature and assume that they satisfy the Gumm equations. Such algebras are automatically idempotent.

Definition 5.2. By a *Jónsson ideal* in an algebra $\mathbf{A} = \langle A; J_0, \dots, J_{2m}, Q\rangle$ we mean a subuniverse U of $\mathbf{A}$ such that whenever $0 \le i \le 2m$, $u, v \in U$ and $a \in A$ then $J_i(u,a,v) \in U$.

Lemma 5.3. *Suppose that $\mathbf{A} = \langle A; J_0, \dots, J_{2m}, Q\rangle$ is a nontrivial algebra satisfying the Gumm equations, and $\mathbb{A} = (A, E)$ is a nicely connected graph over $\mathbf{A}$. Then there exists a non-void proper subuniverse C and a congruence θ of $\mathbf{A}$ such that*

- *$Q(x,y,z)$ is a Maltsev term for $\mathbf{A}/\theta$,*
- *if $\theta = 1_A$ then the induced graph $\mathbb{C} = (C, E \cap C^2)$ is nicely connected.*

Proof. In the same way as in the first and second paragraph of the proof of Theorem 4.4, we can find a Jónsson ideal B of $\mathbf{A}$ such that $\mathcal{N}_{\mathbb{A}}(B, 1) = A$ and the induced subgraph $\mathbb{B} = (B, E \cap B^2)$ contains a cycle. Let C be the union of all the cycles in $\mathbb{B}$ and let $\mathbb{C} = (C, E \cap C^2)$ be the induced subgraph.

Claim 1. *C is a Jónsson ideal of $\mathbf{A}$.*

First we show that C is a subuniverse. If c_0, c_1, c_2 belong to cycles in $\mathbb{B}$ then we can concatenate those cycles with themselves to arrange that all have the same length, say $c_0 = c_0^0, \dots, c_m^0 = c_0$ is a cycle, $c_1 = c_0^1, \dots, c_m^1 = c_1$ is another, $c_2 = c_0^2, \dots, c_m^2 = c_2$ is a third. Let $R(x,y,z)$ be any of the basic operations of $\mathbf{A}$. Then we have the cycle $\{R(c_i^0, c_i^1, c_i^2) : 0 \le i \le m\}$ in $\mathbb{B}$, showing that $R(c_0, c_1, c_2) \in C$. Thus C is a subuniverse.

Let $c, d \in C$ and $a \in A$ and let $J(x,y,z)$ be one of the Jónsson operations $J_i(x,y,z)$. Using the fact that $c, d \in C$ and that $\mathbb{A}$ is strongly connected we can find, for a large m, cycles $c = c_0, \dots, c_m = c$ and $d = d_0, \dots, d_m = d$ and $a = a_0, \dots, a_m = a$ with c_i and d_i belonging to B. Then the cycle $\{J(c_i, a_i, d_i) : 0 \le i \le m\}$ lies in $\mathbb{B}$, since B is a Jónsson ideal of $\mathbf{A}$, showing that $J(c, a, d) \in C$.

Denote by $\mathbf{C}$ the subalgebra of $\mathbf{A}$ with subuniverse C. Denote by $\sim_{\mathbb{C}}$ the equivalence relation over C whose classes are the strong components of $\mathbb{C}$. Thus for $x, y \in C$ we have that $x \sim_{\mathbb{C}} y$ iff x and y both belong to one cycle in $\mathbb{C}$ (or equivalently, in $\mathbb{B}$).

Next we define a binary relation γ on C. For $x, y \in C$, let $x \; \gamma \; y$, if $x \sim_{\mathbb{C}} y$ and $x \xrightarrow{n,\mathbb{F}} y$ for some n divisible by $\zeta(\mathbb{F})$, where $\mathbb{F}$ is the strong component of $\mathbb{C}$ containing x (and y). Observe that $\gamma = 1_C$ is equivalent to the fact that $\mathbb{C}$ is nicely connected.

Claim 2. *γ is a congruence relation on the algebra* $\mathbf{C}$.

Using Lemma 3.1, it is easy to demonstrate that γ is an equivalence relation over C. Moreover, if $(x, y) \in \gamma$ and $\mathbb{F}$ is the strong component of $\mathbb{C}$ containing x and y, then $x \xrightarrow{n,\mathbb{F}} y$ for all large n congruent to 0 modulo $\zeta(\mathbb{F})$. Thus, if $(x_i, y_i) \in \gamma$, $0 \leq i \leq 2$, then there is $n > 0$, divisible by $\zeta(\mathbb{H})$ for every strong component $\mathbb{H}$ of $\mathbb{C}$, such that $x_i \xrightarrow{n,\mathbb{C}} y_i$ and $y_i \xrightarrow{n,\mathbb{C}} x_i$ for each $i \in \{0, 1, 2\}$. If $R(x, y, z)$ is one of the fundamental operations of $\mathbf{A}$, then clearly $R(x_0, x_1, x_2) \xrightarrow{n,\mathbb{C}} R(y_0, y_1, y_2)$ and $R(y_0, y_1, y_2) \xrightarrow{n,\mathbb{C}} R(x_0, x_1, x_2)$, so that

$$R(x_0, x_1, x_2) \; \gamma \; R(y_0, y_1, y_2) \; \text{ and } \; R(y_0, y_1, y_2) \; \gamma \; R(x_0, x_1, x_2).$$

Claim 3. *For every $c, d \in C$ we have $Q(c, d, d) \; \gamma \; c$.*

Let M be the least common multiple of $\{\zeta(\mathbb{H}) \mid \mathbb{H}$ is a strong component of $\mathbb{C}\}$. Using the fact that $c, d \in C$ and that $\mathbb{A}$ is nicely connected, by Lemma 3.1 we find that there is a $k > 0$ such that $c \xrightarrow{kM,\mathbb{C}} c$, $d \xrightarrow{kM,\mathbb{C}} d$, $c \xrightarrow{kM,\mathbb{A}} d$ and $d \xrightarrow{kM,\mathbb{A}} c$. Then, since C is a Jónsson ideal in $\mathbf{A}$, we have

$$c \xrightarrow{kM,\mathbb{C}} c = J_1(c, d, d), \; J_1(c, d, d) \xrightarrow{kM,\mathbb{C}} J_1(c, c, d) = J_2(c, c, d),$$

$$J_2(c, c, d) \xrightarrow{kM,\mathbb{C}} J_3(c, d, d), \ldots, J_{2m-1}(c, c, d) \xrightarrow{kM,\mathbb{C}} J_{2m}(c, d, d) = Q(c, d, d).$$

Hence we have $c \xrightarrow{2mkM,\mathbb{C}} Q(c, d, d)$. Similarly, $Q(c, d, d) \xrightarrow{2mkM,\mathbb{C}} c$. It follows that $(c, Q(c, d, d)) \in \gamma$.

Claim 4. *Suppose that $a \in A$, $c, d \in C$, $c', d' \in B$, $n \geq 0$, and $c \xrightarrow{n,\mathbb{B}} c' \xrightarrow{\mathbb{A}} a$, $d \xrightarrow{n,\mathbb{B}} d' \xrightarrow{\mathbb{A}} a$. Then $(c, d) \in \gamma$.*

To see this, use the previous claim and its proof. For a large $k > n$, we have

$$c \xrightarrow{kM,\mathbb{C}} Q(c, d, d), \; Q(c, d, d) \xrightarrow{kM,\mathbb{C}} c,$$

$$d \xrightarrow{kM,\mathbb{C}} Q(d, c, c) \; \text{ and } \; Q(d, c, c) \xrightarrow{kM,\mathbb{C}} d.$$

There are paths $c = c_0, c_1, \ldots, c_n = a$ and $d = d_0, d_1, \ldots, d_n = a$ in $\mathbb{A}$ with $c_i, d_i \in B$ for $i < n$. There is a cycle in $\mathbb{C}$ of length $2kM$ with c and $Q(c, d, d)$ as antipodes. Let $c, u_1, \ldots, u_n$ be a segment of this cycle. This yields a path

$$Q(d, c, c), Q(d_1, c_1, u_1), Q(d_2, c_2, u_2), \ldots, Q(d_{n-1}, c_{n-1}, u_{n-1}), Q(a, a, u_n) = u_n$$

entirely inside B. Likewise, there is a cycle of length $2kM$ in $\mathbb{C}$ with d and $Q(d, c, c)$ as antipodes. Letting $d, v_1, \dots, v_n$ be a segment of this cycle, we get a path

$$Q(c, d, d), Q(c_1, d_1, v_1), Q(c_2, d_2, v_2), \dots, Q(c_{n-1}, d_{n-1}, v_{n-1}), Q(a, a, v_n) = v_n$$

entirely inside B. Putting the two displayed paths together with the other paths given by the relations $c \xrightarrow{kM,\mathbb{C}} Q(c, d, d)$, etc, we get a cycle in B (and therefore entirely within C) containing $c, Q(c, d, d), d, Q(d, c, c)$, in which the segment from c to d and the segment from d to c each have length divisible by kM. This shows that indeed $(c, d) \in \gamma$.

Now we define the relation θ on A by $(x, y) \in \theta$ iff there is $n > 0$, $c \in C$ and $b, b' \in B$ such that $c \xrightarrow{n,\mathbb{B}} b \xrightarrow{\mathbb{A}} x$ and $c \xrightarrow{n,\mathbb{B}} b' \xrightarrow{\mathbb{A}} y$.

Claim 5. *$\theta|_C = \gamma$. In particular, if $\theta = 1_A$, then $\mathbb{C}$ is nicely connected.*

Suppose that $(c, d) \in \gamma$. Let $\mathbb{F}$ be the strong component of $\mathbb{C}$ containing c and d. There is a large m divisible by $\zeta(\mathbb{F})$ such that $c \xrightarrow{m,\mathbb{F}} d$ and $c \xrightarrow{m,\mathbb{F}} c$. Clearly this yields that $(c, d) \in \theta$.

Conversely, let $c, d \in C$ and $(c, d) \in \theta$. Say we have paths

$$e = u_0, u_1, \dots, u_n = c, \qquad e = v_0, v_1, \dots, v_n = d,$$

with $u_i, v_i \in B$ for $i < n$ and $e \in C$. We can assume that n is divisible by M (defined above) and that $c \xrightarrow{n,\mathbb{C}} c$ and $d \xrightarrow{n,\mathbb{C}} d$. There is a path $d = f_0, f_1, \dots, f_n = d$ in $\mathbb{C}$. Now we have the path

$$d = Q(e, e, f_0), Q(u_1, v_1, f_1), \dots, Q(u_n, v_n, f_n) = Q(c, d, d),$$

lying inside B. Since, by Claim 3, $Q(c, d, d)$ is γ related to c, we can obtain a path from d to c in B of length divisible by M. Similarly, there is such a path from c to d. These paths combined show that $(c, d) \in \gamma$.

If $\theta = 1_A$, then $\gamma = 1_C$ which is equivalent to the fact that $\mathbb{C}$ is nicely connected.

Claim 6. *θ is a congruence relation on $\mathbf{A}$.*

For transitivity, suppose that $(x, y), (y, z) \in \theta$. Thus we have $m, n \geq 1$, $c, d \in C$ and paths

$$c = t_0, \dots, t_m = x,\ c = u_0, \dots, u_m = y,$$
$$d = v_0, \dots, v_n = y,\ d = w_0, \dots, w_n = z,$$

in $\mathbb{A}$ with $t_i, u_i \in B$ when $i < m$ and $v_i, w_i \in B$ when $i < n$. Clearly, we can arrange that $m = n$. By Claim 4 $(c, d) \in \gamma$, thus by Claim 5 $(c, d) \in \theta$, so there is $e \in C$ and paths

$$e = r_0, \dots, r_k = c;\ e = s_0, \dots, s_k = d$$

in $\mathbb{A}$ with $r_i, s_i \in B$. Thus we have the paths

$$e = r_0, \dots, r_k = c = t_0, \dots, t_n = x;\ e = s_0, \dots, s_k = d = w_0, \dots, w_n = z$$

showing that $(x, z) \in \theta$.

Symmetry and reflexivity of θ over A are easy, as is the admissibility under the operations $J_0, \ldots, J_{2m}, Q$.

Claim 7. *For every $x \in A$ there is $y \in C$ with $(x, y) \in \theta$.*

The proof of this claim is almost immediate. The fact that $\mathcal{N}_{\mathbb{A}}(B, 1) = A$ gives a sequence $x = x_0 \leftarrow x_1 \leftarrow \cdots \leftarrow x_n \leftarrow \cdots$ with $x_i \in B$ for $i > 0$. There is $j > 0$ and $n > 0$ with $x_j = x_{j+n}$. Thus $\{x_j, \ldots, x_{j+n-1}\} \subseteq C$ and there are $y_0 \leftarrow \cdots \leftarrow y_j = x_j$ with $y_0, \ldots, y_j$ in $\{x_j, \ldots, x_{j+n-1}\}$. Clearly, $(x, y_0) \in \theta$.

From Claims 3 and 7 it easily follows that $Q(x, y, y) \; \theta \; x$ for all $x, y \in A$. Therefore $Q(x, y, z)$ is a Maltsev term for $\mathbf{A}/\theta$. □

Now we are ready to prove the main theorem of this paper.

Theorem 5.4. *If $\mathbf{A}$ is a finite algebra in a congruence modular variety, then for every prime integer p greater than $|A|$, $\mathbf{A}$ possesses a cyclic term of arity p.*

Proof. Striving for a contradiction, take a minimal counterexample with respect to $|A|$. As usual, we can assume that $\mathbf{A} = \langle A; J_0, \ldots, J_{2m}, Q \rangle$, thus $\mathbf{A}$ is idempotent. Then $\mathbf{A}$ is simple by Lemma 2.5. If $\mathbf{A}$ is Abelian, then it is Maltsev (an Abelian algebra in a congruence-modular variety), and we have a contradiction with Theorem 5.1. Thus $\mathbf{A}$ is a non-Abelian simple algebra. It follows that $\mathbf{A}$ is neutral, i.e., for all congruences θ, ψ on $\mathbf{A}$ we have $[\theta, \psi] = \theta \cap \psi$, where $[\theta, \psi]$ denotes the commutator.

From Freese and McKenzie [7], we know that if $\mathbf{A}$ is a finite neutral algebra with Gumm terms, then every finite subdirect power of $\mathbf{A}$ is neutral, and its congruence lattice is distributive. Therefore we can apply Lemma 4.1 to obtain a nicely connected graph $\mathbb{G} = (G, E)$ over a subdirect power $\mathbf{G} \leq \mathbf{A}^{p-1}$ with no loops such that for every proper subuniverse C of $\mathbf{G}$ the induced graph $\mathbb{C} = (C, E \cap H^2)$ is not nicely connected.

An application of Lemma 5.3 now gives us a proper subuniverse C and a congruence θ on $\mathbf{G}$ such that the algebra $\mathbf{G}/\theta$ is Maltsev, and if $\theta = 1_G$ then the induced graph $\mathbb{C} = (C, E \cap C^2)$ is nicely connected. But $\mathbb{C}$ can not be nicely connected (see the paragraph above), thus $\theta < 1_G$. We use now that $\mathbf{G}$ is a subdirect power of the neutral algebra $\mathbf{A}$. Using the distributive law in the congruence lattice of $\mathbf{G}$, we get that $\theta \vee \eta_i \neq 1_G$ for some i, where η_i is the kernel of the ith projection. Since η_i is a co-atom in the congruence lattice ($\mathbf{A}$ is simple), then $\theta \leq \eta_i$. This implies that $\mathbf{A}$ is Maltsev, as it is a homomorphic image of $\mathbf{G}/\theta$, a contradiction with Theorem 5.1. □

Remark 5.5. Recently, the first, second and fifth authors of this paper have shown that every nicely connected graph over an algebra in a variety omitting type **1** has a loop (see [1]). This provides, together with Lemma 4.1, a generalization of Theorem 4.5 in which the word "distributive" can be replaced by "join-semidistributive."

References

[1] 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 J. Comp. **38**, 1782–1802 (2009)

[2] Brauer, A., Shockley, J.E.: On a problem of Frobenius. J. Reine. Angew. Math. **211**, 215–220 (1962)

[3] Bulatov, A.A., Krokhin, A., Jeavons, P.G.: Constraint satisfaction problems and finite algebras. In: Proc. of the 27th Int. Colloquium on Automata, Languages and Programming (ICALP). Lecture Notes in Computer Science, vol. 1853, pp. 272–282. Springer (2000)

[4] Burris, S., Sankappanavar, H.P.: A Course in Universal Algebra. Graduate Texts in Mathematics, vol. 78. Springer, New York (1981)

[5] Carvalho, C., Dalmau, V., Marković, P., Maróti, M.: CD(4) has bounded width. Algebra Universalis **60**, 293–307 (2009)

[6] Feder, T., Vardi, M.Y.: The computational structure of monotone monadic SNP and constraint satisfaction: a study through Datalog and group theory. SIAM J. Computing **28**, 57–104 (1998)

[7] Freese, R., McKenzie, R.: Commutator Theory for Congruence Modular Varieties. London Mathematical Society Lecture Note Series, vol. 125. Cambridge University Press, Cambridge (1987)

[8] Gumm, H.P.: Geometrical methods in congruence modular varieties. Mem. Amer. Math. Soc. **45**, 286 (1983)

[9] Hobby, D., McKenzie, R.: The Structure of Finite Algebras. Contemporary Mathematics, vol. 76. American Mathematical Society, Providence (1988)

[10] Kiss, E.W., Valeriote, M.: On tractability and congruence distributivity. Logical Methods in Computer Science **3** (2007)

[11] Maltsev, A.I.: On the general theory of algebraic systems. Mat. Sb. N.S. **35**(77), 3–20 (1954) (Russian)

[12] Maltsev, A.I.: On the general theory of algebraic systems. Amer. Math. Soc. Transl. (2) **27**, 125–142 (1963) (English translation of Maltsev, 1954)

[13] Maróti, M., McKenzie, R.: Existence theorems for weakly symmetric operations. Algebra Universalis **59**, 463–489 (2008)

[14] McKenzie, R., McNulty, G., Taylor, W.: Algebras, Lattices, Varieties, vol. 1. Wadsworth & Brooks/Cole, Monterey (1987)

Libor Barto

Department of Algebra, Charles University, Prague, Czech Republic
e-mail: jetel@matfyz.cz

Marcin Kozik

Department of Theoretical Computer Science, Jagiellonian University, Krakow, Poland, and Eduard Čech Center, Prague, Czech Republic
e-mail: kozik@tcs.uj.edu.pl

Miklós Maróti

Bolyai Institute, University of Szeged, Szeged, Hungary
e-mail: mmaroti@math.u-szeged.hu

Ralph McKenzie

Department of Mathematics, Vanderbilt University, Nashville, USA
e-mail: ralph.n.mckenzie@vanderbilt.edu

Todd Niven

Eduard Čech Center, Prague, Czech Republic
e-mail: niven@karlin.mff.cuni.cz