International Journal of Algebra and Computation
© World Scientific Publishing Company

# ON ALGEBRAS WITH MANY SYMMETRIC OPERATIONS

CATARINA CARVALHO
*University of Hertfordshire*
*Hatfield, AL10 9AB, UK*
*c.carvalho2@herts.ac.uk*

ANDREI KROKHIN
*Durham University*
*Durham, DH1 3LE, UK*
*andrei.krokhin@durham.ac.uk*

Received (Day Month Year)
Accepted (Day Month Year)

Communicated by [editor]

An $n$-ary operation $f$ is called *symmetric* if, for all permutations $\pi$ of $\{1,\ldots,n\}$, it satisfies the identity $f(x_1,x_2,\ldots,x_n) = f(x_{\pi(1)},x_{\pi(2)},\ldots,x_{\pi(n)})$. We show that, for each finite algebra $\mathcal{A}$, either it has symmetric term operations of all arities or else some finite algebra in the variety generated by $\mathcal{A}$ has two automorphisms without a common fixed point. We also show this two-automorphism condition cannot be replaced by a single fixed-point-free automorphism.

*Keywords*: symmetric operation; automorphism; variety

Mathematics Subject Classification 2010: 08A05; 08A70; 03C05

## 1. Introduction

The study of algebras with particular types of term operations has always been a subject of interest in the field of Universal Algebra [10,15], and it has boomed since its connections with the complexity of Constraint Satisfaction Problems (CSPs) was discovered (see, e.g. [7,9]). Many complexity classification results for the CSP are based on algebraic dichotomies (of independent interest) of the form: either an algebra $\mathcal{A}$ has term operations satisfying certain “nice” identities or else some finite algebra in the variety generated by $\mathcal{A}$ has some “bad” compatible relational structure, often of a simple form (see [2,4,7,9,18]). Such structures are the forbidden structures for these “nice” term operations. We give several examples of such algebraic dichotomies in Section 3.

In this paper, we identify the forbidden structures for having *symmetric* operations (of all arities) as term operations. A symmetric operation is an operation that is invariant under any permutation of arguments. Such operations have recently been used in the algebraic approach to the CSP [16], they characterise the CSPs solvable by a natural algorithm based on linear programming. One intended use of our forbidden structures is in proofs of computational hardness results, such as non-existence of certain robust algorithms [12,16], for CSPs that cannot be solved by linear programming.

## 2. Definitions

The definitions given in this section are standard. A *vocabulary* $\tau$ is a finite set of relation symbols $R_1, \ldots, R_k$ or arities $r_1, \ldots, r_k \geq 1$. A $\tau$-structure $\mathbf{B}$ consists of a finite set $B$, called the *universe* of $\mathbf{B}$, and a relation $R^{\mathbf{B}} \subseteq B^r$ for every relation symbol $R \in \tau$ where $r$ is the arity of $R$.

A *homomorphism* from a $\tau$-structure $\mathbf{A}$ to a $\tau$-structure $\mathbf{B}$ is a mapping $h : A \to B$ such that for every $r$-ary $R \in \tau$ and every $(a_1, \ldots, a_r) \in R^{\mathbf{A}}$, we have $(h(a_1), \ldots, h(a_r)) \in R^{\mathbf{B}}$. We write $\mathbf{A} \to \mathbf{B}$ if there is a homomorphism from $\mathbf{A}$ to $\mathbf{B}$.

The *constraint satisfaction (or homomorphism) problem* for a structure $\mathbf{B}$ is testing whether a given structure $\mathbf{A}$ admits a homomorphism to $\mathbf{B}$. This problem is denoted by CSP($\mathbf{B}$), and can be identified with the class of all structures $\mathbf{A}$ such that $\mathbf{A} \to \mathbf{B}$.

Let $f$ be an $n$-ary operation on $B$, and $R$ a relation of $\mathbf{B}$. We say that $f$ is a *polymorphism* of $R$ if, for any tuples, $\bar{a}_1, \ldots, \bar{a}_n \in R$, the tuple obtained by applying $f$ componentwise to $\bar{a}_1, \ldots, \bar{a}_n$ also belongs to $R$. In this case, $R$ is said to be *invariant* under $f$, or *compatible* with $f$. Furthermore, $f$ is a *polymorphism of* $\mathbf{B}$ if it is a polymorphism of each relation in $\mathbf{B}$. It is easy to check that the $n$-ary polymorphisms of $\mathbf{B}$ are precisely the homomorphisms from the $n$-th direct power $\mathbf{B}^n$ to $\mathbf{B}$. We denote by Pol($\mathbf{B}$) the set of all polymorphisms of $\mathbf{B}$.

A *finite algebra* is a pair $\mathcal{A} = (A, F)$ where $A$ is a finite set and $F$ is a family of operations of finite arity on $A$. The *term operations* of $\mathcal{A}$ are the operations obtained from $F$ and the projections by superposition. A *variety* is a class of (indexed) algebras closed under taking homomorphic images, subalgebras, and direct products. The *variety generated by* $\mathcal{A}$, var($\mathcal{A}$), consists of all homomorphic images of subalgebras of direct powers of $\mathcal{A}$. As usual, $HS(\mathcal{A})$ denotes the class of all homomorphic images of subalgebras of $\mathcal{A}$. From each relational structure $\mathbf{B}$, one can obtain an algebra $\mathcal{A}_{\mathbf{B}} = (B, \mathrm{Pol}(\mathbf{B}))$, by taking as operations on the universe $B$ the polymorphism of all relations in $\mathbf{B}$. A structure $\mathbf{B}'$ with universe $A$ is said to be *compatible* with an algebra $\mathcal{A} = (A, F)$ if every operation in $F$ is a polymorphism of $\mathbf{B}'$ (equivalently, each relation in $\mathbf{B}'$ is the universe of a subalgebra of the corresponding power of $\mathcal{A}$).

The notion of a polymorphism plays the key role in the algebraic approach to the CSP. The polymorphisms of a structure are known to determine the complexity of CSP($\mathbf{B}$) as well as definability of (the complement of) CSP($\mathbf{B}$) in various logics (see [6,18]).

We now define several types of operations that will be used in this paper.

- An $n$-ary operation $f$ is called *idempotent* if it satisfies the identity $f(x,\dots,x)=x$.
- An $n$-ary operation $f$ is called *cyclic* if it satisfies the identity
$$f(x_1,x_2,\dots,x_n)=f(x_2,x_3,\dots,x_n,x_1);$$
- An $n$-ary operation $f$ is called *symmetric* if it satisfies the identity
$$f(a_1,a_2,\dots,a_n)=f(a_{\pi(1)},a_{\pi(2)},\dots,a_{\pi(n)})$$
for all permutations $\pi$ of $\{1,\dots,n\}$;
- An $n$-ary operation $f$ is called *totally symmetric* if $f(x_1,\dots,x_n)=f(y_1,\dots,y_n)$ whenever $\{x_1,\dots,x_n\}=\{y_1,\dots,y_n\}$. If, in addition, $f$ is idempotent then we say that it is a TSI operation.
- An $n$-ary ($n\geq 3$) operation is called a *weak near-unanimity (WNU)* operation if it is idempotent and it satisfies the identities
$$f(y,x,\dots,x,x)=f(x,y,\dots,x,x)=\dots=f(x,x,\dots,x,y).$$
- A *Mal'tsev* operation is a ternary operation $f$ satisfying
$$f(x,x,y)=f(y,x,x)=y.$$

More of the universal-algebraic background can be found in [10,15].

## 3. Some algebraic dichotomies

We will now describe some known algebraic dichotomy results and indicate where they are used in the study of CSPs. It is known [7] that it is enough to classify only problems CSP($\mathbf{B}$) such that the corresponding algebra $\mathcal{A}_{\mathbf{B}}$ is idempotent, i.e. all of its operations are idempotent. This explains why most of the dichotomies concern only idempotent algebras.

(i) For a finite idempotent algebra $\mathcal{A}$, either $\mathcal{A}$ has a cyclic operation of some arity (equivalently, var($\mathcal{A}$) satisfies a non-trivial Mal'tsev condition), or else the ternary relation $\{(0,0,1),(0,1,0),(1,0,0)\}$ is compatible with some (2-element) algebra in $HS(\mathcal{A})$ [2].

It is known that, for a structure $\mathbf{B}$, if the (idempotent) algebra $\mathcal{A}_{\mathbf{B}}$ satisfies the latter condition then CSP($\mathbf{B}$) is **NP**-complete [7]. The Algebraic Dichotomy Conjecture states that if $\mathcal{A}_{\mathbf{B}}$ satisfies the former condition then CSP($\mathbf{B}$) is tractable [2,7].

(ii) For a finite idempotent algebra $\mathcal{A}$, either $\mathcal{A}$ has WNU operations of almost all arities (equivalently, var($\mathcal{A}$) is congruence meet-semidistributive), or else there exists an algebra $\mathcal{B}$ in $HS(\mathcal{A})$ and an Abelian group structure on the base set of $\mathcal{B}$ such that the relation $\{(x,y,z): x+y=z\}$ is compatible with $\mathcal{B}$ [18,19].

It is known that the former condition, for the algebra $\mathcal{A}_{\mathbf{B}}$, implies that CSP($\mathbf{B}$) is definable in the logic programming language Datalog [4] (and also admits a robust algorithm [3]), while the latter condition, which intuitively says that CSP($\mathbf{B}$) can encode systems of linear equations, implies the absence of these nice properties [13,12].

(iii) For a finite idempotent algebra $\mathcal{A}$, either $\mathcal{A}$ has ternary term operations from Theorem 9.11 of [15] (equivalently, var($\mathcal{A}$) is congruence join-semidistributive), or else there exists an algebra $\mathcal{B}$ in $HS(\mathcal{A})$ such that at least one of the relations $\{(x,y,z) : x+y = z\}$ (as above) and $\{0,1\}^3\setminus\{(1,1,0)\}$ is compatible with $\mathcal{B}$ [18].

The former condition, for the algebra $\mathcal{A}_{\mathbf{B}}$, is conjectured to imply that CSP($\mathbf{B}$) is definable in linear Datalog [18] (which roughly means that CSP($\mathbf{B}$) can be reduced to the Digraph Reachability problem) and belongs to the complexity class **NL**, while the latter condition, which intuitively says that CSP($\mathbf{B}$) can encode systems of linear equations or Horn 3-Sat, implies non-definability in linear Datalog and non-membership in **NL** (modulo complexity-theoretic assumptions) [18].

(iv) For a finite idempotent algebra $\mathcal{A}$, either $\mathcal{A}$ has a Mal'tsev operation as a term operation (equivalently, var($\mathcal{A}$) is congruence permutable), or else some binary reflexive and non-symmetric relation is compatible with a finite algebra $\mathcal{V}(\mathcal{A})$ [14].

The latter condition was used in [5] to prove hardness of the counting version of CSP($\mathbf{B}$), and in [8] to prove hardness of a version of CSP($\mathbf{B}$) with an additional global constraint.

## 4. Forbidden structures for many symmetric operations

Since the presence of many symmetric operations plays a role in the study of CSPs, it is natural to try to find (simple enough) forbidden structures for this algebraic condition.

For a permutation $\pi$ on $A$, let $\pi^\circ$ denote the graph of $\pi$, i.e. $\pi^\circ = \{(a, \pi(a)) \mid a \in A\}$. In the next two sections we will deal with graphs of permutations compatible with algebras. Note that $\pi^\circ$ is compatible with an algebra $\mathcal{A}$ if and only if $\pi$ is an automorphism of $\mathcal{A}$.

The following is a slightly weakened Proposition 2.1 of [1].

**Proposition 4.1.** *Let $\mathcal{A}$ be a finite algebra.*

- *Either $\mathcal{A}$ has cyclic term operations of all arities,*
- *or else there is a finite algebra $\mathcal{B}$ in* var($\mathcal{A}$) *with a fixed-point-free automorphism.*

Since any symmetric operation is cyclic, the latter condition in Proposition 4.1 is sufficient to forbid the existence of symmetric term operations of all arities. Could it also be necessary, at least for algebras of the form $\mathcal{A}_{\mathbf{B}}$? We will show that it is not, but a small variation of it is such a condition.

**Theorem 4.2.** *Let $\mathcal{A}$ be a finite algebra.*

- *Either $\mathcal{A}$ has symmetric term operations of all arities,*
- *or else there is a finite algebra $\mathcal{B}$ in* $\mathrm{var}(\mathcal{A})$ *that has two automorphisms without a common fixed point. Furthermore, one of the automorphisms can be chosen to have order two.*

**Proof.** It is easy to see that if $f$ is an $n$-ary symmetric term operation of $\mathcal{A}$, and hence of every algebra in $\mathrm{var}(\mathcal{A})$, then, for any algebra $\mathcal{B}$ in $\mathrm{var}(\mathcal{A})$ with universe $\{b_1, \dots, b_n\}$, the element $f(b_1, \dots, b_n)$ is a fixed point of every automorphism of $\mathcal{B}$.

Assume now that $\mathcal{A}$ does not have a symmetric operation of arity $n$. Let $\mathcal{F}$ be the free $n$-generated algebra in the variety $\mathrm{var}(\mathcal{A})$, with free generators $x_1, x_2, \dots, x_n$. Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be the subalgebras of $\mathcal{F} \times \mathcal{F}$ generated by the tuples

$$\mathcal{A}_1 = \langle\ (x_1, x_2), (x_2, x_1), (x_3, x_3), \dots, (x_n, x_n)\ \rangle$$

$$\mathcal{A}_2 = \langle\ (x_1, x_2), (x_2, x_3), (x_3, x_4), \dots, (x_{n-1}, x_n), (x_n, x_1)\ \rangle.$$

Since $x_1, \dots, x_n$ are the free generators of $\mathcal{F}$, the universes of $\mathcal{A}_1$ and $\mathcal{A}_2$ can be thought of as graphs of permutations on the universe of $\mathcal{F}$ (and hence correspond to automorphisms of $\mathcal{F}$). The automorphism corresponding to $\mathcal{A}_1$ has order two. If these permutations share a fixed point then there exist $n$-ary operations $f_1$ and $f_2$ and an element $a$ in $\mathcal{F}$ such that

$$\begin{aligned}&f_1((x_1, x_2), (x_2, x_1), (x_3, x_3), \dots, (x_n, x_n)) = \\ &f_2((x_1, x_2), (x_2, x_3), \dots, (x_{n-1}, x_n), (x_n, x_1)) = (a, a).\end{aligned}$$

This implies that $f_1 = f_2$ and, moreover, $f_1(x_1, x_2, x_3, \dots, x_n) = f_1(x_2, x_1, x_3, x_4, \dots, x_n) = f_1(x_2, x_3, \dots, x_n, x_1)$, and so $f_1$ is symmetric. Hence we have an $n$-ary symmetric operation in $\mathcal{A}$, a contradiction. ■

The classes of algebras appearing in Proposition 4.1 and Theorem 4.2 are different, as our next result shows. Hence, graphs of fixed-point-free permutations do not form a complete set of forbidden structures for the existence of symmetric term operations of all arities.

Let $\mathbf{K} = (K; R, S)$ be the structure with domain

$$K = \{0, 1, 2, \dots, 9, 10, \overline{01}, \overline{02}, \overline{03}, \overline{04}, \overline{12}, \overline{13}, \overline{14}, \overline{23}, \overline{24}, \overline{34}\},$$

and binary relations $R$ and $S$ that are graphs of the following permutations $r$ and $s$, respectively,

$$r = (0\ 1\ 2)(5\ 6\ 7)(8\ 9\ 10)(\overline{12}\ \overline{02}\ \overline{01})(\overline{04}\ \overline{14}\ \overline{24})(\overline{13}\ \overline{23}\ \overline{03}),$$

$$s = (1\ 4)(2\ 3)(5\ 6)(7\ 8)(\overline{34}\ \overline{12})(\overline{02}\ \overline{03})(\overline{01}\ \overline{04})(\overline{24}\ \overline{13}).$$

It will be often convenient to think of $\mathbf{K}$ as of two graphs as depicted in Figure 1, one directed, $R$ (represented by the solid lines), and one undirected, $S$ (represented by the dotted lines), on the same set of vertices $K$. Then fixed points of permutations correspond to loops in the graphs. To simplify notation, for elements of the form $\overline{xy}$ we assume the convention that $\overline{xy} = \overline{yx}$.

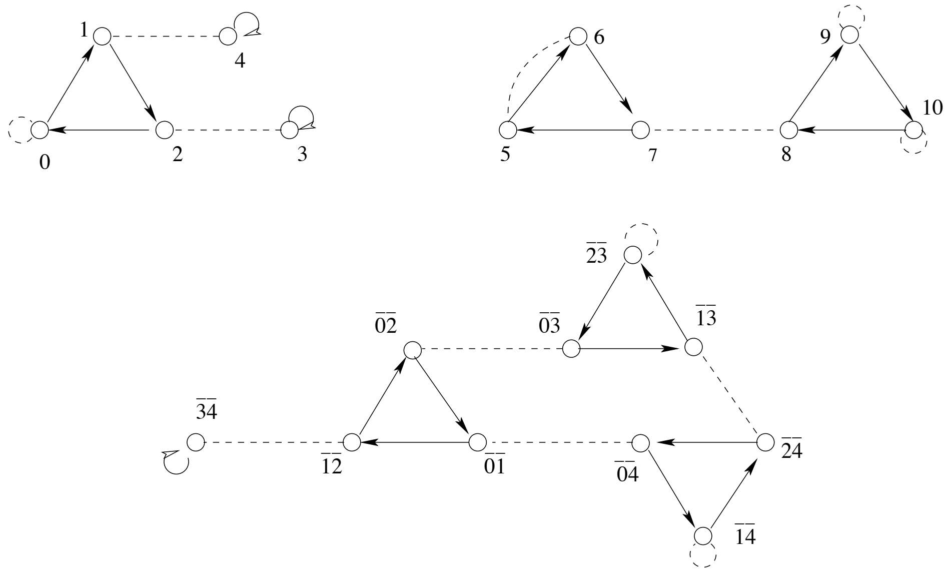

Fig. 1. Relational structure **K**

**Theorem 4.3.** *The structure* **K** *has cyclic polymorphisms of all arities, but no symmetric polymorphism of arity 5.*

**Proof.** For a contradiction, suppose that $f$ is a 5-ary symmetric operation that preserves both $R$ and $S$. Since $f$ is symmetric we know that $f(0,1,2,3,4) = f(1,2,0,3,4) = f(0,4,3,2,1)$. We have that $(0,1),(1,2),(2,0),(3,3),(4,4) \in R$ and $(0,0),(1,4),(2,3),(3,2),(4,1) \in S$. It follows that $f(0,1,2,3,4)$ is a common loop in $R$ and $S$, which does not exist, a contradiction. The proof that **K** has cyclic polymorphisms of all arities occupies the next section. ■

We used computer-assisted search in the process of finding the structure $K$, but the search was not designed to find the smallest structure with required properties, so we do not know whether $K$ is smallest. We do know that this example of structure is tight in the sense that the existence of cyclic operations of all arities imply the existence of symmetric operations of arities up to 4.

**Lemma 4.4.** *If an algebra $\mathcal{A}$ has cyclic term operations of arities 2 and 3 then it also has symmetric term operations of arities up to 4.*

**Proof.** Let $s_2, c_3$ be cyclic operations of arities 2 and 3 respectively. Clearly $s_2$ is symmetric, and it is easy to check that the operation

$$s_3(x,y,z) = s_2(c_3(x,y,z), c_3(y,x,z))$$

is a 3-ary symmetric operation.

Now, the 4-ary operation $t(x,y,z,w) = s_2(s_2(x,y), s_2(z,w))$ satisfies the following identities

$$\begin{aligned} t(x,y,z,w) &= t(y,x,z,w) = t(x,y,w,z) = t(y,x,w,z) \\ &= t(z,w,x,y) = t(z,w,y,x) = t(w,z,x,y) = t(w,z,y,x). \end{aligned}$$

It then follows that the operation

$$s_4(x,y,z,w) = s_3(t(x,y,z,w), t(x,w,y,z), t(x,z,y,w))$$

is symmetric. ∎

**Remark 4.5.** The condition of having totally symmetric operations of all arities has also played a role in the study of the CSP. Such operations characterise the so-called CSPs of width 1, i.e. CSPs solvable by the arc-consistency algorithm [11,13]. It was claimed in [16] that this condition is equivalent to the one of having many symmetric operations, but a flaw was discovered in the proof (as acknowledged on R. O'Donnell's webpage), and a counter-example to the claim was recently found by G. Kun [17, Example 99]: a very simple structure that has symmetric polymorphisms of all arities, but no ternary totally symmetric polymorphism.

## 5. Proof of Theorem 4.3

We make use of two results that have been proved for algebras, that can naturally be applied to relational structures.

**Proposition 5.1.** *[1, Proposition 2.2] For a finite algebra $\mathcal{A}$ the following hold:*

1. *If $\mathcal{A}$ has an $n$-ary cyclic term then it has a $k$-ary cyclic term for all $k > 1$ divisor of $n$.*
2. *If $\mathcal{A}$ has an $n$-ary and an $m$-ary cyclic term, then it also has an $mn$-ary cyclic term.*

**Proposition 5.2.** *[2, Theorem 4.1] Let $\mathcal{A}$ be a finite algebra. The following are equivalent*

- *$\mathcal{A}$ has a cyclic term;*
- *$\mathcal{A}$ has a cyclic term of arity $p$, for every prime $p > |A|$.*

It follows from Propositions 5.1 and 5.2 that it is enough to show that $\mathbf{K}$ has cyclic polymorphisms of arity $p$ for all prime $p < 21$. We will define partial cyclic operations of prime arities on $K$, and then show by induction that $\mathbf{K}$ is preserved by cyclic operations of arities up to 21.

Consider the following partition of $K$: $C_1 = \{0, \dots, 4\}$, $C_2 = \{5, \dots 10\}$, and $C_3 = \{\overline{01}, \dots, \overline{34}\}$; blocks $C_1$ and $C_3$ are depicted in Fig. 2 and Fig. 3, respectively. In these figures the filled lines represent the arcs of $R$ and the dotted lines the (undirected) edges of $S$.

We start by defining partial cyclic operations $c_p(x_1, \dots, x_p)$ for all prime $p < 21$ and $x_1, \dots, x_p$ all belonging to the same block. These operations do not necessarily preserve the blocks but preserve $R$ and $S$. Then, using these operations, we show, by induction on $n$, that $R$ and $S$ are preserved by cyclic operations of arity $n$, for all $n = 2, \dots, 21$. Recall that, for elements of the form $\overline{xy}$, we assume the convention that $\overline{xy} = \overline{yx}$.

(1) *Definition of $c_p(x_1, \dots, x_p)$ with $x_1, \dots, x_p$ all distinct and belonging to the same block:*
We assume that $x_1, \dots, x_p$ are all distinct, so when they belong to $C_1$ or $C_2$ we just need to define $c_p$ for $p \le 5$, and when they belong to $C_3$ we define $c_p$ for $p \le 7$.

We define the operation $c_2$ to act symmetrically on all blocks, i.e once we define it on a tuple $(x, y)$ the definition is the same on the tuple $(y, x)$. For distinct $x, y \in C_1$ we let $c_2(x, y) = \overline{xy}$; for distinct $x, y \in C_3$ we define

$$c_2(x,y) = \begin{cases} a \text{ if } x = \overline{ab}, y = \overline{ac} \text{ for some } a \in C_1 \\ e \text{ if } x = \overline{ab}, y = \overline{cd}, \text{ and } C_1 = \{a, b, c, d, e\}; \end{cases}$$

and for distinct $x, y \in C_2$ we define it as shown in Fig. 2: $c_2(5, 6) = c(7, 8) = c_2(9, 10) = 0,\ c_2(5, 7) = c_2(6, 10) = c_2(8, 9) = 2$ and so on.

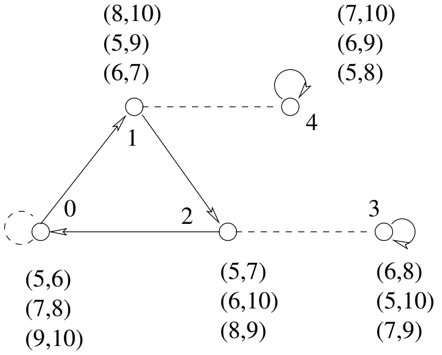

Fig. 2. Operation $c_2$ maps $C_2$ to $C_1$

It is worth noting that operation $c_2$ and below $c_3$ and $c_5$ are defined on the block $C_3$ by going over all isomorphism types of graphs on $\{0,1,2,3,4\}$ that have $2,3$ and $5$ edges, respectively.

To check that $c_2$, as defined, preserves relations $R$ and $S$ we can start with any two elements of $C_1$ and follow their images in $C_3$, moving along elements connected first by $R$ and then by $S$. Indeed component $C_3$ appeared by defining a binary symmetric relation on $C_1$. For elements of $C_2$ we can check that adjacency in both $R$ and $S$ is preserved by $c_2$ by checking all mapping in Figure 2. Operation $c_2$ sends any two elements of $C_3$ to an element of $C_3$, we can also follow adjacency in block $C_3$ in Figure 1; e.g. we have for example $(\overline{01},\overline{12}),(\overline{14},\overline{24}) \in R$ and $c_2(\overline{01},\overline{14}) = 1, c_2(\overline{12},\overline{24}) = 2$ and we can see that $(1,2) \in R$.

We define operation $c_3$ to also act symmetrically on all elements, i.e once we define it on a tuple $(x,y,z)$ the operation takes the same value on any tuple obtained by arbitrarily permuting $x,y,z$. For distinct $x,y,z \in C_1$ we define $c_3(x,y,z) = c_2(u,v)$ where $\{u,v\} = C_1 \backslash \{x,y,z\}$; when $x,y,z \in C_3$ are all distinct, we let

$$c_3(x,y,z) = \begin{cases} \overline{de} \text{ if } & x = \overline{ab},\ y = \overline{bc},\ z = \overline{ac}, \\ \overline{ae} \text{ if } & x = \overline{ab},\ y = \overline{ac},\ z = \overline{ad}, \\ a \text{ if } & x = \overline{ab},\ y = \overline{ac},\ z = \overline{de}, \\ e \text{ if } & x = \overline{ab},\ y = \overline{bc},\ z = \overline{ad}; \end{cases}$$

and in $C_2$ we define $c_3$ as shown in Fig. 3: $c_3(5,6,7) = c_3(8,9,10) = \overline{34}$, and so on.

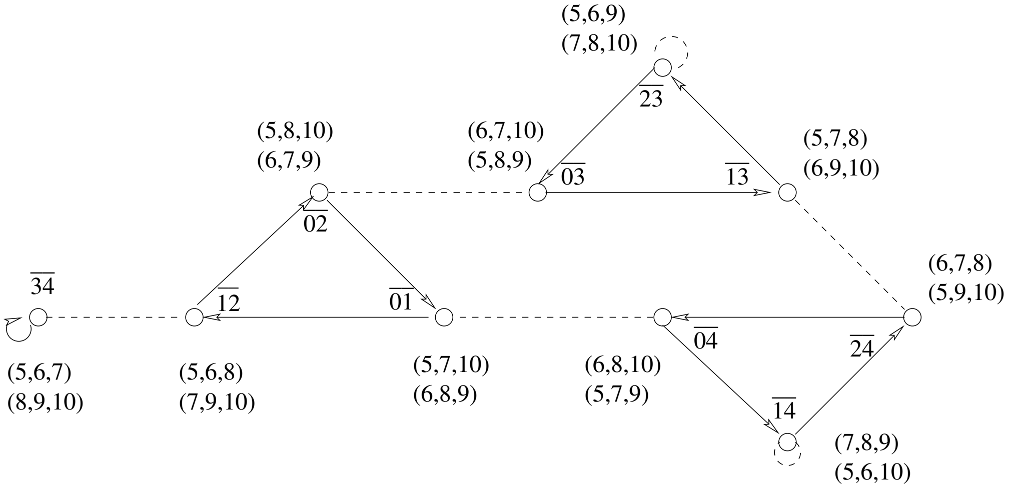

Fig. 3. Operation $c_3$ maps $C_2$ to $C_3$

To check that $c_3$, as defined, preserves relations $R$ and $S$ for any two elements of $C_1$ follows immediately from the fact that $c_2$ preserves $R$ and $S$, for any two elements of $C_2$ we can follow the image of the elements in Fig. 3; if we consider $c_3$ acting on elements of $C_3$ the idea is that triples of elements considered in each of the 4 cases of $c_3$ are connected, via $R$ and $S$, to triples considered in the same case type, and we can then check that the relations are preserved by following the pictures of components $C_3$ and $C_1$, e.g. we have

$$\begin{aligned}
&(\overline{03},\overline{13}),(\overline{13},\overline{23}),(\overline{01},\overline{12})\in R \text{ and } (c_3(\overline{03},\overline{13},\overline{01}),c_3(\overline{13},\overline{23},\overline{12}))=(\overline{24},\overline{04})\in R;\\
&(\overline{01},\overline{12}),(\overline{02},\overline{01}),(\overline{03},\overline{13})\in R \text{ and } (c_3(\overline{01},\overline{02},\overline{03}),c_3(\overline{12},\overline{01},\overline{13}))=(\overline{04},\overline{14})\in R\\
&(\overline{01},\overline{04}),(\overline{02},\overline{03}),(\overline{34},\overline{12})\in S \text{ and } (c_3(\overline{01},\overline{02},\overline{34}),c_3(\overline{04},\overline{03},\overline{12}))=(0,0)\in S\\
&(\overline{01},\overline{04}),(\overline{12},\overline{34}),(\overline{03},\overline{02})\in S \text{ and } (c_3(\overline{01},\overline{12},\overline{03}),c_3(\overline{04},\overline{34},\overline{02}))=(4,1)\in S.
\end{aligned}$$

We define the operation $c_5$ to be cyclic in $C_1$ and symmetric on the remaining blocks, i.e once we define an operation on a tuple $(x_1,\ldots,x_5)$ it takes the same value on all tuples obtained from cycling permuting $x_1,\ldots,x_5$, and if $x_1,\ldots,x_5$ belong to $C_2$ or $C_3$ the operation also takes the same value on the tuples obtained by arbitrarily permuting $x_1,\ldots,x_5$. When $x,y,z,u,v\in C_2$ are all distinct, we define $c_5(x,y,z,u,v)=w$ where $C_2=\{x,y,z,u,v,w\}$; and for distinct $x,y,z,u,v\in C_3$ we define

$$c_5(x,y,z,u,v)=\begin{cases}
a & \text{if } x=\overline{ab},y=\overline{ac},z=\overline{ad},u=\overline{ae},v=\overline{ce}\\
a & \text{if } x=\overline{ab},y=\overline{cd},z=\overline{eb},u=\overline{bd},v=\overline{ad}\\
e & \text{if } x=\overline{ab},y=\overline{cd},z=\overline{cb},u=\overline{bd},v=\overline{ad}\\
e & \text{if } x=\overline{ab},y=\overline{cd},z=\overline{cb},u=\overline{bd},v=\overline{ae}\\
c_5(a,b,c,d,e) & \text{if } x=\overline{ab},y=\overline{bc},z=\overline{cd},u=\overline{de},v=\overline{ae}
\end{cases}$$

where $C_1=\{a,b,c,d,e\}$; in $C_1$ we define

$$c_5(0,1,2,4,3)=5,\quad c_5(0,4,3,1,2)=6,\quad c_5(0,1,4,3,2)=7,$$
$$c_5(0,4,1,2,3)=8,\quad c_5(0,2,4,1,3)=9,\quad c_5(0,1,3,2,4)=10,$$

and to extend $c_5$ to the rest of $C_1$, we think of the tuple $(x,y,z,u,v)$ as the permutation $(xyzuv)$. It is then easy to see that $(xyzuv)$ is an $i^{th}$ power, with $i=0,1,\ldots,4$, of exactly one of six permutations corresponding to the tuples for which $c_5(x,y,z,u,v)$ was defined above. We then define $c_5(x,y,z,u,v)$ to be the same as $c_5$ applied to the corresponding tuple, e.g. $(02314)=(01243)^2$ and so $c_5(0,2,3,1,4)=5$.

Finally, for distinct $x_1,\ldots,x_7\in C_3$ we define $c_7(x_1,\ldots,x_7)=c_3(a,b,c)$, where $\{a,b,c\}=C_3\backslash\{x_1,\ldots,x_7\}$.

We now extend these operations to elements $x_1,\ldots,x_p$ belonging to the same component but not necessarily distinct.

(2) *Definition of $c_p(x_1,\ldots,x_p)$ with $x_1,\ldots,x_p$ not all distinct and belonging to the same block, and $p$ any prime number:*
For convenience, we define $c_1(x)=x$ for all $x\in V$.

**Claim 5.3.** *Let $p$ be any prime number, and $x_1,\ldots,x_p$ be elements from the same block of $K$. If $|\{x_1,\ldots,x_p\}|\geq 5$ then there exists $k=1,\ldots,p$ such that at most 4 elements of $\{x_1,\ldots,x_p\}$ appear exactly $k$ times in $x_1,\ldots,x_p$.*

**Proof.** For all $i = 1, \ldots, p$, let $N_i$ be the (possibly empty) set of elements that appear exactly $i$ times in $x_1, \ldots, x_p$. Note that $|N_1| < p$, since $x_1, \ldots, x_p$ are not all distinct, and $|N_p| = 0$ because $|\{x_1, \ldots, x_p\}| \geq 5$. We have $p = \sum_{i=1}^{p} i|N_i|$, which implies that there are at least two $i$'s for which $N_i$ is non-empty, for $p$ is prime. Let $j_1$ and $j_2$ be the smallest and largest $i$, respectively, for which $N_i$ is non-empty. We show that at least one of $N_{j_1}$, $N_{j_2}$ has at most 4 elements. Suppose, for a contradiction, that $|N_{j_1}| \geq 5$ and $|N_{j_2}| \geq 5$. Then the $x_i$'s must all come from $C_3$. The set $N_{j_1} \cup N_{j_2}$ contains 10 different elements, i.e. all elements of $C_3$. It follows all the other sets $N_i$ are empty, and $p = 5j_1 + 5j_2$, a contradiction. ■

We then define $c_p(x_1, \ldots, x_p) = c_j(y_1, \ldots, y_j)$, where $j \leq 4$, and either $\{x_1, \ldots, x_p\} = \{y_1, \ldots, y_j\}$ or, when $|\{x_1, \ldots, x_p\}| \geq 5$, $y_1, \ldots, y_j$ are the (at most 4) elements repeated exactly $k$ times mentioned in Claim 5.3 (and $k$ is the smallest such value). Note that the elements $y_1, \ldots, y_j$ are all distinct and come from the same block, so $c_j(y_1, \ldots, y_j)$ is already defined. Indeed, $c_j(y_1, \ldots, y_j)$ is defined to be symmetric in (1) for $j \leq 3$. Also by (1) and using (the proof of) Lemma 4.4 we know that there exists a symmetric operation $s_4$ defined on elements $x_1, \ldots, x_4$ all distinct and belonging to the same block. It follows that $c_p$ acts on $x_1, \ldots, x_p$ as a symmetric operation.

We now show that these partial operations preserve the relations $R$ and $S$.

**Claim 5.4.** *Let $x_1, \ldots, x_p \in K$ be elements from the same partition block. If $(x_1, y_1), \ldots, (x_p, y_p) \in R$ (respectively $\in S$) then $(c_p(x_1, \ldots, x_p), c_p(y_1, \ldots, y_p)) \in R$ (respectively $\in S$).*

**Proof.** First note that $y_1, \ldots, y_p$ also belong to the same block. If $x_1, \ldots, x_p$ are all distinct, then $c_p(x_1, \ldots, x_p)$ was defined in (1), and it is not hard to check directly that these partial operations preserve $R$ and $S$. Note that whenever we have a pattern in the repetition of elements in $x_1, \ldots, x_p$, this pattern is the same in $y_1, \ldots, y_p$. For example if $x_1 = x_2$ and $x_3, \ldots, x_p$ are all distinct then $y_1 = y_2$ and $y_3, \ldots, y_p$ are all distinct. This immediately implies that the partial operations defined in (2) preserve $R$ and $S$, as a consequence of the partial operations defined in (1) also preserving them. ■

We now extend the operations define above to elements not belonging to the same block, at the same time as, by induction on $n$, defining cyclic operations, $c'_n$, of arity $n$ for all $n < 21$, that preserve the relations in $\mathbf{K}$. For $n = 2$ we define an idempotent cyclic operation $c'_2$ as follows

$$c'_2(x, y) = \begin{cases} x & \text{if } x \in C_i, y \in C_j,\ i < j \\ y & \text{if } x \in C_i, y \in C_j,\ i > j \\ c_2(x, y) & \text{if } x, y \in C_i, \end{cases}$$

with $i, j = 1, 2, 3$ and $c_2$ as defined in (1) and (2). It is easy to check that $c'_2$ preserves both $R$ and $S$.

Now, assume that $R$ and $S$ are preserved by cyclic operations, $c'_n$ for all $n < k$. If $k$ is not prime, then $k = mq$ and we know, as in [1], that $c'_k$ can be obtained by composing $c'_m$ and $c'_q$ as follows

$$c'_k(x_1, \dots, x_k) = c'_m(c'_q(x_1, \dots, x_q), \dots, c'_q(x_{k-q+1}, \dots, x_k)).$$

By the inductive hypothesis, $c'_q$ and $c'_m$ preserve $R$ and $S$, so $c'_k$ also preserves these relations. If $k$ is prime we define

$$c'_k(x_1, \dots, x_k) = \begin{cases} c_k(x_1, \dots, x_k) \text{ if } x_1, \dots, x_k \in C_i, \quad (i = 1, 2, 3), \\ c'_m(x_1, \dots, x_m) \text{ if } \{x_1, \dots, x_m\} = C_1 \cap \{x_1, \dots, x_k\} \neq \emptyset, \\ c'_m(x_1, \dots, x_m) \text{ if } \{x_1, \dots, x_m\} = C_2 \cap \{x_1, \dots, x_k\} \text{ and} \\ \qquad\qquad C_1 \cap \{x_1, \dots, x_k\} = \emptyset \end{cases}$$

that is: if all elements $x_1, \dots, x_k$ belong to the same block then we already know from (1) and (2) that there is a cyclic (partial) operation, $c_k$, defined on them that preserves $R$ and $S$; if not all elements belong to the same block then we choose the elements in $x_1, \dots, x_k$ that belong to $C_1$ (or $C_2$ if no element belongs to $C_1$) and apply to them the corresponding operation of smaller arity, which we know exists by the inductive hypothesis. Since the blocks are disjoint and have no arcs connecting them, $c'_k$ clearly preserves both $R$ and $S$. Theorem 4.3 is proved.

## 6. Conclusion

We have described the forbidden structures for the existence of symmetric term operations in a finite algebra. We have also shown that the classes of finite algebras having cyclic operations of all arities and symmetric operations of all arities are not the same. In fact, the algebra $\mathcal{A}_{\mathbf{K}}$ that separates these classes can easily be shown to generate an arithmetical variety.

It is an interesting open question whether Theorem 4.2 can be strengthened by requiring the algebra $\mathcal{B}$ in var($\mathcal{A}$) (that has two automorphisms without a common fixed point) to belong to $HS(\mathcal{A})$. This strengthening could help in the study of complexity (more specifically, robust algorithms) for constraint satisfaction problems [12]. Even obtaining an upper bound on the number $n$ such that $\mathcal{B}$ can be found in $HS(\mathcal{A}^n)$ would be interesting, since such a bound would imply decidability of the existence of symmetric term operations in a finite algebra (and hence decidability of the problem of recognising CSPs solvable by linear programming), which is currently an open question.

## References

[1] L. Barto, M. Kozik, M. Maróti and T. Niven. Congruence modularity implies cyclic terms for finite algebras, *Algebra Universalis*, 61 (3), 365–380, 2009.

[2] L. Barto and M. Kozik Absorbing subalgebras, cyclic terms and the constraint satisfaction problem *Logical Methods in Computer Science* 8 (1:07), 1–26, 2012.

[3] L. Barto and M. Kozik Robust satisfiability of constraint satisfaction problems *STOC'12*, 931–940, 2012.

[4] L. Barto and M. Kozik Constraint satisfaction problem solvable by local consistency methods *Journal of the ACM*, 61 (1), Article 3, 2014.

[5] A. Bulatov and V. Dalmau. Towards a Dichotomy Theorem for Counting CSP. *Information and Computation* 205(5): 651–678 (2007).

[6] A. Bulatov, A. Krokhin and B. Larose. Dualities for constraint satisfaction problems, In: *Complexity of Constraints*, LNCS 5250, 93–124, 2008.

[7] A. Bulatov, P. Jeavons and A. Krokhin, Classifying the complexity of constraints using finite algebras, *SIAM J. Comput.* 34 (3), 720–742, 2005.

[8] A. Bulatov and D. Marx, The complexity of global cardinality constraints, *Logical Methods in Computer Science*, 6(4), 2010.

[9] A. Bulatov and M. Valeriote. Recent results on the algebraic approach to the CSP, In:*Complexity of Constraints*, 68–92, 2008.

[10] S. Burris and H.P. Sankappanavar. *A Course in Universal Algebra* Springer-Verlag, Berlin-New York, 1981.

[11] V. Dalmau and J. Pearson. Set Functions and Width 1, In *CP'99*, vol.1713 of LNCS, 159–173, 1999.

[12] V. Dalmau and A. Krokhin. Robust satisfiability for CSPs: hardness and algorithmic results *ACM Transactions on Computation Theory*, 5 (4), Article 15, 2013.,

[13] T. Feder and M. Vardi. The computational structure of monotone monadic SNP and constraint satisfaction: A study through Datalog and group theory *SIAM Journal on Computing* 28 (1), 57–104, 1998

[14] J. Hagemann and A. Mitschke, On $n$-permutable congruences, *Algebra Universalis* 3, 8–12, 1973.

[15] D. Hobby and R. McKenzie, *The Structure of Finite Algebras,* Contemporary Mathematics Series Vol. 76, American Mathematical Society, Providence, RI, 1991.

[16] G. Kun, R. O'Donnell, S.Tamaki, Y. Yoshida and Y. Zhou. Linear programming, width-1 CSPs, and robust satisfaction, *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, 484–495, 2012

[17] G. Kun. and M. Szegedy A new line of attack on the dichotomy conjecture, *European Journal of Combinatorics* 52 (B) 338–367, 2016

[18] B. Larose and P. Tesson. Universal Algebra and Hardness Results for Constraint Satisfaction Problems, *Theoret. Comput. Sci.* 410, 1629-1647, 2009.

[19] M. Maróti and R. McKenzie. Existence theorems for weakly symmetric operations, *Algebra Universalis* 59 (2008), no. 3-4, 463-489.