CANCELLATION AMONG FINITE UNARY ALGEBRAS

Miroslav Ploščica and Miron Zelina

Abstract. We show that a unary algebra is cancellable among finite unary algebras if and only if it contains a one–element subalgebra.

1. Introduction

We are interested in the following problem: for which algebras $\mathbf{C}$ the condition $\mathbf{A} \times \mathbf{C} \cong \mathbf{B} \times \mathbf{C}$ implies $\mathbf{A} \cong \mathbf{B}$?

Let us call an algebra $\mathbf{C}$ cancellable in a class $\mathcal{K}$ of algebras if $\mathbf{C} \in \mathcal{K}$ and $\mathbf{C}$ has the following property: for all $\mathbf{A}$, $\mathbf{B} \in \mathcal{K}$, if $\mathbf{A} \times \mathbf{C} \cong \mathbf{B} \times \mathbf{C}$, then $\mathbf{A} \cong \mathbf{B}$. We call $\mathbf{C}$ cancellable among finite algebras if $\mathbf{C}$ is cancellable in the class of all finite algebras of its similarity type.

A characterization of algebras cancellable among finite algebras has not been known for any nontrivial similarity type (see [4] for a survey). However, there are some characterization results for relational structures (see [1], [3]). In case of algebras, the best known result is the following theorem due to L. Lovász:

Theorem 1. (See [2], [4].) *Every finite algebra having a one–element subalgebra is cancellable among finite algebras.* □

The aim of this paper is to prove the converse of this theorem for unary algebras with an arbitrary number of operations. To make the paper accesible to a wider audience, we explain here the basic concepts for unary algebras.

Let F be a set of unary operational symbols. By a unary algebra $\mathbf{A} = (A, F)$ we mean a set A (called the underlying set) on which unary operations $f^{\mathbf{A}}$ are defined for all $f \in F$. If $\mathbf{A}$ is understood, we usually write f instead of $f^{\mathbf{A}}$. We admit the cases $A = \emptyset$ and $F = \emptyset$.

A congruence on $\mathbf{A} = (A, F)$ is an equivalence relation $\sim$ on the set A satisfying the following compatibility condition for each $f \in F$: if $x \sim y$ then $f(x) \sim f(y)$. For any such congruence we can form the factor algebra $\mathbf{A}/\!\sim = (A/\sim, F)$, whose underlying set $Asim$ is the set of all equivalence classes (blocks) of $\sim$ and the operations are defined in a natural way: $f([x]) = [f(x)]$. (Here $[y]$ means the block containing y.)

The product of algebras $\mathbf{A} = (A, F)$, $\mathbf{B} = (B, F)$ is the unary algebra $\mathbf{A} \times \mathbf{B} = (A \times B, F)$ whose underlying set is the Cartesian product $A \times B$ and the operations are defined by $f^{\mathbf{A}\times\mathbf{B}}(x, y) = (f^{\mathbf{A}}(x), f^{\mathbf{B}}(y))$.

An isomorphism between $\mathbf{A}$ and $\mathbf{B}$ is a bijective mapping $\varphi : A \longrightarrow B$ preserving each $f \in F$, i.e. satisfying $\varphi(f^{\mathbf{A}}(x)) = f^{\mathbf{B}}(\varphi(x))$ for every $x \in A$. If there is an

Supported by Grant GA–SAV 362/92

isomorphism between $\mathbf{A}$ and $\mathbf{B}$, we say that $\mathbf{A}$ and $\mathbf{B}$ are isomorphic and write $\mathbf{A} \cong \mathbf{B}$.

For any set X, $\mathcal{P}(X)$ denotes the set of all subsets of X and $|X|$ means the cardinality of X. For any positive integer t, $\underline{t}$ denotes the set $\{0, \ldots, t-1\}$. For a composition of mappings we adopt the convention that $f \circ g(x) = f(g(x))$.

We assume throughout that $\mathbf{C} = (C, F)$ is a finite unary algebra (i.e. the set C is finite) without any one-element subalgebra. Our aim is to construct two nonisomorphic algebras $\mathbf{A}$ and $\mathbf{B}$ of the same type as $\mathbf{C}$ such that $\mathbf{A} \times \mathbf{C} \cong \mathbf{B} \times \mathbf{C}$.

Let F^* be the set of all mappings $C \longrightarrow C$ that can be obtained by a composition of some finite number of operations from $\{f^{\mathbf{C}} \ : \ f \in F\}$ (including the identity mapping ι_C, which is the composition of the empty set of functions).

We say that an element $x \in C$ is f-cyclic (for $f \in F^*$), if $f^k(x) = x$ for some positive integer k. If this condition is not fulfilled, we say that x is f-acyclic. An element x is called cyclic, if it is f-cyclic for every $f \in F^*$. If x is not cyclic, it is called acyclic. It is easy to see that if x is f-cyclic, then so is $f(x)$. Let $\mathfrak{C}(\mathbf{C})$ be the family of all subsets of C which are closed under all $f \in F^*$ and consist of cyclic elements. The family $\mathfrak{C}(\mathbf{C})$ is clearly closed under set-theoretical union and therefore contains the greatest element (with respect to set inclusion). This greatest element will be called the core of $\mathbf{C}$ and denoted by $\mathrm{Core}(\mathbf{C})$. It is clear that any $f \in F^*$ restricted to $\mathrm{Core}(\mathbf{C})$ is a permutation. In fact, $\mathrm{Core}(\mathbf{C})$ is the largest subset of C on which all the operations are permutations. Let us remark that the case $\mathrm{Core}(\mathbf{C})= \emptyset$ is possible.

Hence, every element of $\mathrm{Core}(\mathbf{C})$ is cyclic. However, there might be cyclic elements that do not belong to $\mathrm{Core}(\mathbf{C})$. Consider the following example. Let $A = \{a, b, c\}$ and define $f, g, h, k \ : \ A \longrightarrow A$ by $f(a) = c$, $f(b) = f(c) = a$, $g(a) = a$, $g(b) = g(c) = b$, $h = f \circ f$, $k = g \circ f$. It is not difficult to check that the set $\{f, g, h, k, \iota\}$ is composition closed (ι is the identity mapping), the algebra $\mathbf{A} = (A, \{f, g, h, k, \iota\})$ has an empty core and the element $a \in A$ is cyclic. The following assertion provides an alternative definition of $\mathrm{Core}(\mathbf{C})$.

Lemma 1. $\mathrm{Core}(\mathbf{C}) = \{x \in C \ : \ f(x)$ *is cyclic for every* $f \in F^*\}$

Proof. Clearly, any $x \in \mathrm{Core}(\mathbf{C})$ satisfies the above condition. Conversely, suppose that $x \notin \mathrm{Core}(\mathbf{C})$. Let $X = \{f(x) \ : \ f \in F*^{\}}$. Then X is closed under all $f \in F^*$. Since F^* contains the identity mapping, we have $x \in X$ and hence $X \nsubseteq \mathrm{Core}(\mathbf{C})$. By the definition of $\mathrm{Core}(\mathbf{C})$, X must contain an acyclic element. □

We define an equivalence relation $\approx$ on $\mathrm{Core}(\mathbf{C})$ by the rule $a \approx b$ if and only if $b = f(a)$ for some $f \in F^*$. This is indeed an equivalence relation, since each $f \in F^*$ restricted to $\mathrm{Core}(\mathbf{C})$ is a permutation of a finite rank. Let $C_1, \ldots, C_s$ be the equivalence classes of $\approx$. (We will call them cyclic components of $\mathbf{C}$.) Notice that F^* acts transitively on each cyclic component. Set

$$n = 2.|C_1| \ldots |C_s|.$$

If $\mathrm{Core}(\mathbf{C})$ is empty then $n = 2$. Further, let us set

$$E = \{\, (X, Y) : X \subseteq Y \subseteq C, |Y \setminus X| = 1 \,\}.$$

Hence E can be regarded as the set of all oriented edges in the Hasse diagram (covering graph) of $\mathcal{P}(C)$ (the ordered set of all subsets of C). Denote by C^* the

set of all finite sequences of elements from C (including the empty sequence). For any
$\mathbf{c} =< c_1, \ldots, c_t >\in C^*$ we define its path as a sequence $\pi(\mathbf{c}) =< p_0, \ldots, p_t >$ of subsets of C, determined by the following rule:

$$p_j = \{\, c \in C : c \text{ occurs odd number of times in the sequence } < c_1, \ldots, c_j > \}.$$

It is easy to see that $\pi(\mathbf{c})$ is indeed a path in the Hasse diagram of $\mathcal{P}(C)$. The starting set p_0 equals $\emptyset$, the set p_t is called the terminal set for $\mathbf{c}$. The characteristic of $\mathbf{c}$ is the map $\chi_{\mathbf{c}} : E \to \mathbb{Z}$ (the set of all integers) defined as follows. For each $e \in E$, $e = (A, B)$ set

$$\chi_{\mathbf{c}}(e) = |\{j \in \underline{t} : (A, B) = (p_j, p_{j+1})\}| - |\{j \in \underline{t} : (A, B) = (p_{j+1}, p_j)\}|.$$

Thus $\chi_{\mathbf{c}}(e)$ is the difference between the number of times the path $\pi(\mathbf{c})$ traverses the edge e upwards (from A to B) and the number of times $\pi(\mathbf{c})$ traverses e downwards (from B to A).

For every map $f : C \to C$ we define the associated map $f^* : \mathcal{P}(C) \to \mathcal{P}(C)$ by

$$f^*(X) = \{\, a \in C : \text{ the set } X \cap f^{-1}(a) \text{ has an odd number of elements} \,\}.$$

The motivation for this definition lies in the following easy fact: if $< p_0, \ldots, p_t >$ is the path of $\mathbf{c} =< c_1, \ldots, c_t >$, then $< f^*(p_0), \ldots, f^*(p_t) >$ is the path of $f(\mathbf{c}) =< f(c_1), \ldots, f(c_t) >$.

In the next assertion we express $\chi_{f(\mathbf{c})}$ by means of $\chi_{\mathbf{c}}$. First notice that $(p_j, p_{j+1}) \in E$ does not imply $(f^*(p_j), f^*(p_{j+1})) \in E$; the case $(f^*(p_{j+1}), f^*(p_j)) \in E$ is possible. That is why we need two kinds of "inverse image of $e \in E$". For every $f : C \to C$ and $e \in E$ we set

$$f^{-1}(e)^+ = \{\, (X, Y) \in E : (f^*(X), f^*(Y)) = e \,\},$$
$$f^{-1}(e)^- = \{\, (X, Y) \in E : (f^*(Y), f^*(X)) = e \,\}.$$

Lemma 2. *For every $f : C \to C$, $\mathbf{c} =< c_1, \ldots, c_t >\in C^*$, $e \in E$, the following equality holds:*

$$\chi_{f(\mathbf{c})}(e) = \sum_{x \in f^{-1}(e)^+} \chi_{\mathbf{c}}(x) - \sum_{x \in f^{-1}(e)^-} \chi_{\mathbf{c}}(x).$$

Proof. Clearly,

$$\sum_{x \in f^{-1}(e)^+} \chi_{\mathbf{c}}(x) =$$
$$\sum_{x \in f^{-1}(e)^+} |\{j \in \underline{t} : x = (p_j, p_{j+1})\}| - \sum_{x \in f^{-1}(e)^+} |\{j \in \underline{t} : x = (p_{j+1}, p_j)\}| =$$
$$= |\{j \in \underline{t} : (p_j, p_{j+1}) \in f^{-1}(e)^+\}| - |\{j \in \underline{t} : (p_{j+1}, p_j) \in f^{-1}(e)^+\}| =$$
$$= |\{j \in \underline{t} : (p_j, p_{j+1}) \in E, (f^*(p_j), f^*(p_{j+1})) = e\}| -$$
$$|\{j \in \underline{t} : (p_{j+1}, p_j) \in E, (f^*(p_{j+1}), f^*(p_j)) = e\}|.$$

Similarly,

$$\sum_{x\in f^{-1}(e)^-}\chi_{\mathbf{c}}(x)=|\{j\in \underline{t}:(p_j,p_{j+1})\in E,(f^*(p_{j+1}),f^*(p_j))=e\}|-$$
$$|\{j\in \underline{t}:(p_{j+1},p_j)\in E,(f^*(p_j),f^*(p_{j+1}))=e\}|.$$

Since, for every j, either $(p_j,p_{j+1})\in E$ or $(p_{j+1},p_j)\in E$ we obtain that

$$\sum_{x\in f^{-1}(e)^+}\chi_{\mathbf{c}}(x)-\sum_{x\in f^{-1}(e)^-}\chi_{\mathbf{c}}(x)=$$
$$=|\{j\in \underline{t}:(f^*(p_j),f^*(p_{j+1}))=e\}|-|\{j\in \underline{t}:(f^*(p_{j+1}),f^*(p_j))=e\}|=$$
$$=\chi_{f(\mathbf{c})}(e).\quad\square$$

Let us define an equivalence relation $\sim$ on C^* by $\mathbf{c}\sim\mathbf{d}$ iff $\chi_{\mathbf{c}}(e)\equiv\chi_{\mathbf{d}}(e)\pmod n$ for every $e\in E$.

Lemma 3. *If $\mathbf{c}\sim\mathbf{d}$, then $\mathbf{c}$ and $\mathbf{d}$ have the same terminal set.*

Proof. For any $X\subseteq C$ denote

$$k_{\mathbf{c}}(X)=\sum_{A=X\text{ or }B=X}\chi_{\mathbf{c}}(A,B).$$

Hence, $k_{\mathbf{c}}(X)$ is the number of times the path of $\mathbf{c}$ enters X or leaves X. If $X\neq\emptyset$ and $X\neq p_t$ (the terminal set for $\mathbf{c}$), the number $k_{\mathbf{c}}(X)$ is even, because whenever $\pi(\mathbf{c})$ enters X, it must leave it. If $p_t=\emptyset$, then also $k_{\mathbf{c}}(\emptyset)$ is even, otherwise $k_{\mathbf{c}}(\emptyset)$ and $k_{\mathbf{c}}(p_t)$ are odd. The same holds for the sequence $\mathbf{d}$. From $\mathbf{c}\sim\mathbf{d}$ it follows that $k_{\mathbf{c}}(X)\equiv k_{\mathbf{d}}(X)\pmod n$. Since n is even, we have $k_{\mathbf{c}}(X)\equiv k_{\mathbf{d}}(X)\pmod 2$. Hence, either both terminal sets are equal $\emptyset$ or they are both equal to the only nonempty X with $k_{\mathbf{c}}(X)$ odd. $\square$

It is easy to see that the terminal set for $\mathbf{c}=<c_1,\dots,c_t>$ has an even cardinality if and only if t is even. From this and Lemma 3 we deduce the following consequence.

Lemma 4. *If $\mathbf{c}=<c_1,\dots,c_{2t}>\in C^*$, $\mathbf{d}=<d_1,\dots,d_{2u+1}>\in C^*$, then $\mathbf{c}\sim\mathbf{d}$ does not hold.* $\square$

For every $f\in F$ and $\mathbf{c}=<c_1,\dots,c_t>\in C^*$ we define $f(\mathbf{c})=<f(c_1),\dots,f(c_t)>$. By this way we obtain an algebra $\mathbf{C}^*=(C^*,F)$ of the same type as $\mathbf{C}$.

Lemma 5. *The relation $\sim$ is a congruence of $\mathbf{C}^*$.*

Proof. Let $f\in F$, $\mathbf{c},\mathbf{d}\in C^*$, $\mathbf{c}\sim\mathbf{d}$. Then $\chi_{\mathbf{c}}(e)\equiv\chi_{\mathbf{d}}(e)\pmod n$ for every $e\in E$. We need to show that $\chi_{f(\mathbf{c})}(e)\equiv\chi_{f(\mathbf{d})}(e)\pmod n$ for every $e\in E$. But this follows directly from Lemma 2. $\square$

Denote by A (B) the set of blocks of $\sim$ containing a sequence of even (odd) length. By Lemma 4, the sets A and B are disjoint. It is easy to see that both A and B are closed under all $f\in F$. So we have two algebras $\mathbf{A}=(A,F)$ and $\mathbf{B}=(B,F)$ of the same type as $\mathbf{C}$. They are subalgebras of $\mathbf{C}^*/\!\sim$.

Lemma 6. *Let* $\mathbf{c} =< c_1, \dots, c_t >\in C^*$*,* $\mathbf{d} =< d_1, \dots, d_u >\in C^*$ *be such that* $\mathbf{c} \sim \mathbf{d}$*. Then* $< c_1, \dots, c_t, c >\sim< d_1, \dots, d_u, c >$ *for every* $c \in C$*.*

Proof. Denote $\overline{\mathbf{c}} =< c_1, \dots, c_t, c >$, $\overline{\mathbf{d}} =< d_1, \dots, d_u, c >$. The path of $\overline{\mathbf{c}}$ is obtained from the path $< p_0, \dots, p_t >$ of $\mathbf{c}$ by adding one trasition from p_t to $p_t \cup \{c\}$ (if $c \notin p_t$) or to $p_t \setminus \{c\}$ (if $c \in p_t$). The same holds for $\overline{\mathbf{d}}$ and $\mathbf{d}$. Since $\mathbf{c}$ and $\mathbf{d}$ have the same terminal set and $\mathbf{c} \sim \mathbf{d}$, we deduce that $\overline{\mathbf{c}} \sim \overline{\mathbf{d}}$. □

By a similar reasoning one can show the following assertion.

Lemma 7. *Let* $\mathbf{c} =< c_1, \dots, c_t >\in C^*$*. Then* $< c_1, \dots, c_t, >\sim< c_1, \dots, c_t, c, c >$ *for every* $c \in C$*.* □

Lemma 8. $\mathbf{A} \times \mathbf{C} \cong \mathbf{B} \times \mathbf{C}$.

Proof. For any sequence $\mathbf{c}$ let $[\mathbf{c}]$ denote the block of $\sim$ containing $\mathbf{c}$. We define a mapping $\varphi : \mathbf{A} \times \mathbf{C} \longrightarrow \mathbf{B} \times \mathbf{C}$ as follows. If $[\mathbf{c}] \in \mathbf{A}$, $\mathbf{c} =< c_1, \dots, c_t >$ and $c \in C$, then

$$(*) \qquad \varphi([\mathbf{c}], c) = ([< c_1, \dots, c_t, c >], c).$$

This definition is correct by Lemma 6. The mapping φ is bijective because the same formula (*) defines the inverse mapping $\mathbf{B} \times \mathbf{C} \longrightarrow \mathbf{A} \times \mathbf{C}$. (See Lemma 7.) Finally, it is straightforward to show that φ preserves all $f \in F$. □

It remains to show that $\mathbf{A}$ and $\mathbf{B}$ are not isomorphic. It is easily seen that algebra $\mathbf{A}$ has a one-element subalgebra $(\{[\emptyset]\}, F)$, where $\emptyset$ is the empty sequence. (Of course, the block $[\emptyset]$ contains nonempty sequences as well.) We will prove that $\mathbf{B}$ has no singleton subalgebra.

Suppose to the contrary that $\mathbf{B}$ has a singleton subalgebra $\mathbf{S} = (\{S\}, F)$. Hence S is a block of $\sim$ and for every $\mathbf{c} \in S$, $f \in F$ we have $\mathbf{c} \sim f(\mathbf{c})$. Since the relation $\sim$ is transitive, it follows that $\mathbf{c} \sim f(\mathbf{c})$ holds for every $\mathbf{c} \in S$ and $f \in F^*$. By Lemma 3, all $\mathbf{c} \in S$ have the same terminal set. We denote it by T. Since the sequences in S are of odd lengths, the set T has an odd number of elements. In particular, $T \neq \emptyset$.

Lemma 9. *Let* $\mathbf{c} \in S$*. Then*

(i) *if* $e = (X, Y) \in E$ *is such that* Y *contains an acyclic element, then* $\chi_{\mathbf{c}}(e) \equiv 0 \pmod{n}$*;*
(ii) *the terminal set* T *consists of cyclic elements.*

Proof. Suppose that $a \in Y$ is a f-acyclic element for some $f \in F^*$. Then $a \notin \mathrm{im}(f^k) = f^k(C)$ for a sufficiently large integer k. We have $f^k \in F^*$, $\mathbf{c} \sim f^k(\mathbf{c})$, hence $\chi_{\mathbf{c}}(e) \equiv \chi_{f^k(\mathbf{c})}(e) \pmod{n}$. Since the sequence $f^k(\mathbf{c})$ does not contain the element a, clearly $\chi_{f(\mathbf{c})}(e) = 0$ and $a \notin T$. □

Lemma 10. *For every* $f \in F^*$ *there is* $\mathbf{d} \in S$ *consisting of* f*-cyclic elements. The terminal set* T *is a subset of* Core*(*$\mathbf{C}$*).*

Proof. Clearly, there is an integer k such that $\mathrm{im}(f^k)$ is the set of all f-cyclic elements. If we choose $\mathbf{c} \in S$ arbitrarily, then $\mathbf{d} = f^k(\mathbf{c})$ is the desired sequence.

An element $a \in C$ belongs to T if and only if it occurs an odd number of times in $\mathbf{d}$. Since f permutes the set of all f-cyclic elements and T is the terminal set of both $\mathbf{d}$ and $f(\mathbf{d})$, it follows that f permutes T.

Hence, T is closed under all $f \in F^*$. By Lemma 9, T consists of cyclic elements. According to the definition of core, we have $T \subseteq \mathrm{Core}(\mathbf{C})$. $\square$

Notice that in the case $\mathrm{Core}(\mathbf{C}) = \emptyset$ we already have a contradiction (since $\emptyset \neq T \subseteq \mathrm{Core}(\mathbf{C})$). If the core of $\mathbf{C}$ is not empty, we must go deeper.

Lemma 11. *Let $\mathbf{c} \in S$ and $f \in F^*$. Suppose that $e = (X, Y) \in E$ is such that Y contains f-cyclic elements only. Then $f(e) = (f(X), f(Y)) \in E$ and $\chi_{\mathbf{c}}(e) \equiv \chi_{\mathbf{c}}(f(e)) \pmod n$.*

Proof. The function f is bijective on the set of all f-cyclic elements, hence $f(e) \in E$ holds. We use Lemma 2 with $f(e)$ now playing the role of e. It is not difficult to see that if $x = (U, V) \in f^{-1}(f(e))^+ \cup f^{-1}(f(e))^-$ then either $x = e$ or V contains an f-acyclic element. If V contains an f-acyclic element then by Lemma 9 $\chi_{\mathbf{c}}(x) \equiv 0 \pmod n$. Since $e \in f^{-1}(f(e))^+$, Lemma 2 implies that $\chi_{f(\mathbf{c})}(f(e)) \equiv \chi_{\mathbf{c}}(e) \pmod n$. Since $\mathbf{c} \sim f(\mathbf{c})$, we obtain the desired statement. $\square$

Lemma 12. *Let $\mathbf{c} \in S$ and let $e = (X, Y) \in E$ be such that $X \subseteq \mathrm{Core}(\mathbf{C})$ and $Y \nsubseteq \mathrm{Core}(\mathbf{C})$. Then $\chi_{\mathbf{c}}(e) \equiv 0 \pmod n$.*

Proof. Let $Y \setminus X = \{c\}$. If c is acyclic, the statement follows from Lemma 9. Let c be cyclic. By Lemma 1 there is $f \in F^*$ such that $f(c)$ is acyclic. By Lemma 11 we have

$$\chi_{\mathbf{c}}(e) \equiv \chi_{\mathbf{c}}(f(e)) \pmod n$$

and by Lemma 9, $\chi_{\mathbf{c}}(f(e)) \equiv 0 \pmod n$. $\square$

The last ingredient we need for the proof is the following denotation. For $\mathbf{c} =< c_1, \dots, c_t >\in C^*$ and $G \subseteq C$ put

$$\sigma_{G,\mathbf{c}} = \sum_{X \subseteq G} \sum_{d \in C \setminus G} \chi_{\mathbf{c}}(X, X \cup \{d\}).$$

Hence, $\sigma_{G,\mathbf{c}}$ is the difference between the number of times the path $\pi(\mathbf{c})$ goes from a subset of G to a set outside $\mathcal{P}(G)$ and the number of times $\pi(\mathbf{c})$ goes from a set outside $\mathcal{P}(G)$ to a subset of G.

Lemma 13. *If $\mathbf{c} =< c_1, \dots, c_t >\in C^*$ and $G \subseteq C$ satisfy $p_t \nsubseteq G$, then $\sigma_{G,\mathbf{c}} = 1$.*

Proof. The path $\pi(\mathbf{c})$ starts at $\emptyset \subseteq G$ and terminates at $p_t \nsubseteq G$. The statement just states that every time the path $\pi(\mathbf{c})$ comes from a set outside $\mathcal{P}(G)$ into $\mathcal{P}(G)$ it must later again leave $\mathcal{P}(G)$. $\square$

Now we are ready to prove the theorem. Let $\mathbf{c} \in S$. We have $\emptyset \neq T \subseteq \mathrm{Core}(\mathbf{C})$. Choose a cyclic component $K = C_i$ of $\mathbf{C}$ such that $T \cap K \neq \emptyset$. Let $H = \mathrm{Core}(\mathbf{C}) \setminus K$. Clearly $T \nsubseteq H$. Let us define an equivalence $\approx$ on $K \times \mathcal{P}(H)$ by $(a, X) \approx (a', X')$ if $a' = f(a)$, $X' = f(X)$ for some $f \in F^*$. This is indeed an equivalence relation, since each $f \in F^*$ restricted to $\mathrm{Core}(\mathbf{C})$ is a permutation of a finite rank. Each block L of $\approx$ is a disjoint union $\bigcup_{c \in K} L_c$, where $L_c = \{(a, X) \in L : a = c\}$. If $c, d \in K$, then there is $f \in F^*$ such that $f(c) = d$ and then the assignment $(c, X) \mapsto (f(c), f(X))$ is a bijection $L_c \to L_d$. Hence, all the sets L_c have the same cardinality k and then $|L| = |K|.k$. According to Lemma 11, there exists an integer b such that

$$\chi_{\mathbf{c}}(X, X \cup \{a\}) \equiv b \pmod n$$

for every $(a, X) \in L$. It follows that

$$\sum_{(a,X)\in L} \chi_{\mathbf{c}}(X, X \cup \{a\}) \equiv |K|.k.b \pmod{n}.$$

Summing this for each block L of $\approx$ we find that

$$\sum_{(a,X)\in K\times\mathcal{P}(H)} \chi_{\mathbf{c}}(X, X \cup \{a\}) \equiv |K|.m \pmod{n}$$

for some integer m. Now we compute $\sigma_{H,\mathbf{c}}$. If $X \subset H$ and $a \notin \mathrm{Core}(\mathbf{C})$ then $\chi_{\mathbf{c}}(X, X \cup \{a\}) \equiv 0 \pmod{n}$ by Lemma 12. Hence,

$$\sigma_{H,\mathbf{c}} \equiv \sum_{X\subseteq H} \sum_{d\in K} \chi_{\mathbf{c}}(X, X \cup \{d\}) \equiv |K|.m \pmod{n}.$$

By Lemma 13 we have $\sigma_{H,\mathbf{c}} = 1$, which is a contradiction, since $|K| > 1$ divides n. This completes the proof that **B** has no one-element subalgebra. Therefore, the algebras **A** and **B** are not isomorphic. Together with Lemma 8 and Theorem 1 we obtain the desired result.

Theorem 2. *A finite unary algebra is cancellable among finite algebras if and only if it contains a one-element subalgebra.* □

Finally, let us mention that a similar statement for other than unary algebras is known to be false. By [4, Corollary 2 on p. 323] there are groupoids that are cancellable among finite algebras but do not have one-element subalgebras.

References

[1] R. R. Appleson and L. Lovász: A characterization of cancellable k-ary structures, Period. Math. Hungar. 6, 1975, 17-19.

[2] L. Lovász: Operations with structures, Acta Math. Acad. Sci. Hungar. 18, 1967, 321-328.

[3] L. Lovász: On the cancellation law among finite relational structures, Period. Math. Hungar. 1, no. 2, 1971, 145-156.

[4] R. McKenzie, G. McNulty, W. Taylor: Algebras, Lattices, Varieties, Vol.I, Wadsworth Pub., 1987.

Authors' address: Mathematical Institute, Slovak Academy of Sciences, Grešákova 6, 040 01 Košice, Slovak republic