Acta Sci. Math., 56 (1992), 215—222

Idempotent algebras with transitive automorphism groups

LÁSZLÓ SZABÓ

To Professor Béla Csákány on his 60th birthday

0. Introduction

As a rule a finite algebra with "large" automorphism group is functionally complete. The first general result was found by B. CSÁKÁNY [1], who proved that almost every nontrivial homogeneous algebra (i.e. an algebra whose automorphism group is the full symmetric group) is functionally complete; up to equivalence there are six exceptions. Csákány's theorem was first extended to algebras with triply transitive automorphism groups [9] and later to algebras with doubly transitive automorphism groups [4]; the exceptions are the affine spaces over finite fields. The most general result in this direction is proved in [5] where the structure of functionally incomplete algebras with primitive automorphism groups are completely discribed.

In this paper we investigate finite idempotent algebras with transitive automorphism groups. We show that if an at least three element finite idempotent algebra with transitive automorphism group is simple and has no compatible binary central relation then it is either functionally complete or affine (Theorem 3.1). Moreover, if an at least three element finite idempotent algebra with transitive automorphism group is simple and has a nontrivial semi-projection or a majority function among its term functions then it is functionally complete (Theorem 3.2).

1. Preliminaries

Let A be a fixed universe with $|A|>2$. For any positive integer n let $\mathbf{O}^{(n)}$ denote the set of all n-ary operations on A (i.e. maps $A^n \to A$) and let $\mathbf{O}=\bigcup_{n=1}^{\infty}\mathbf{O}^{(n)}$. An operation from $\mathbf{O}$ is *nontrivial* if it is not a projection. By a *clone* we mean a subset

Research partially supported by Hungarian National Foundation for Scientific Research grant no. 1813.

Received October 4, 1990.

of $\mathbf{O}$ which is closed under superpositions and contains all projections. A ternary operation f on A is a *majority function* if for all $x, y \in A$ we have $f(x, x, y) = f(x, y, x) = f(y, x, x) = x$; f is a *Mal'tsev function* if $f(x, y, y) = f(y, y, x) = x$ for all $x, y \in A$. An n-ary operation t on A is said to be an *i-th semi-projection* ($n \geqq 3, 1 \leqq i \leqq n$) if for all $x_1, \ldots, x_n \in A$ we have $t(x_1, \ldots, x_n) = x_i$ whenever at least two elements among $x_1, \ldots, x_n$ are equal.

A subset $F \subseteqq \mathbf{O}$ as well as the algebra (A, F) is *primal* or *complete* if the clone generated by F (i.e. the set of all term functions of (A, F)) is equal to $\mathbf{O}$; F as well as the algebra (A, F) is *functionally complete* if the clone generated by F together with all constant operations (i.e. the set of all algebraic functions of (A, F)) is equal to $\mathbf{O}$.

We are going to formulate Rosenberg's Completeness Theorem [6], [7] which is the main tool in proving our results. First, however, we need some further definitions.

Let $n, h \geqq 1$. An n-ary operation $f \in \mathbf{O}^{(n)}$ is said to *preserve the h-ary relation* $\varrho \subseteqq A^h$ if ϱ is a subalgebra of the h-th direct power of the algebra $(A; f)$; in other words, f preserves ϱ if for any $n \times h$ matrix with entries in A, whose rows belong to ϱ, the row of column values of f belong to ϱ. Then the set of operations preserving ϱ forms a clone, which is denoted by Pol ϱ. We say that a relation ϱ is a *compatible relation* of the algebra (A, F) if $F \subseteqq \operatorname{Pol} \varrho$. A binary relation is called *nontrivial* if it is distinct from the identity relation and the full relation.

An h-ary relation ϱ on A is called *central* if $\varrho \neq A^h$ and there exists a non-void proper subset C of A such that

(a) $(a_1, \ldots, a_h) \in \varrho$ whenever at least one $a_i \in C$ $(1 \leqq i \leqq h)$;

(b) ϱ is *totally symmetric,* i.e. $(a_1, \ldots, a_h) \in \varrho$ implies $(a_{1\pi}, \ldots, a_{h\pi}) \in \varrho$ for every permutation π of the indices $1, \ldots, h$;

(c) ϱ is *totally reflexive,* i.e. $(a_1, \ldots, a_h) \in \varrho$ if $a_i = a_j$ for some $i \neq j$ $(1 \leqq i, j \leqq h)$.

The set C is called the *center of* ϱ.

Let $h \geqq 3$. A family $T = \{\Theta_1, \ldots, \Theta_m\}$ $(m \geqq 1)$ of equivalence relations on A is called *h-regular* if each Θ_i $(1 \leqq i \leqq m)$ has exactly h blocks and $\Theta_T = \Theta_1 \cap \ldots \cap \Theta_m$ has exactly h^m blocks (i.e. the intersection $\bigcap_{i=1}^{m} B_i$ of arbitrary blocks B_i of Θ_i $(i = 1, \ldots, m)$ is nonempty). The relation determined by T is

$$\lambda_T = \{(a_1, \ldots, a_h) \in A^h \colon a_1, \ldots, a_h \text{ are not pairwise incongruent}$$

$$\text{modulo } \Theta_i \text{ for all } i \ (1 \leqq i \leqq m)\}.$$

Note that h-regular relations are both totally reflexive and totally symmetric.

Now we are in the position to state Rosenberg's Theorem:

Theorem A (I. G. ROSENBERG [6], [7]). *A finite algebra* $\mathbf{A}=(A, F)$ *is primal if and only if* $F \subseteq \mathrm{Pol}\, \varrho$ *for no relation of any of the following six types:*

(1) *a bounded partial order;*

(2) *a binary relation* $\{(a, a\pi) | a \in A\}$ *where* π *is a permutation of* A *with* $|A|/p$ *cycles of the same length* p *(*p *is a prime number);*

(3) *a quaternary relation* $\{(a_1, a_2, a_3, a_4) \in A^4 | a_1+a_2=a_3+a_4\}$ *where* $(A; +)$ *is an elementary abelian p-group (*p *is a prime number);*

(4) *a nontrivial equivalence relation;*

(5) *a central relation;*

(6) *a relation determined by an h-regular family of equivalence relations.*

Let B be a finite set with $|B| \geqq 3$, and let $m>1, n \geqq 1$, $M=\{1, \dots, m\}$, $N=\{1, \dots, n\}$. An n-ary *wreath operation* on B^m is an operation w associated to permutations p_i of B $(i=1, \dots, m)$, and maps $r\colon M \to N$, $s\colon M \to M$, as follows: For $x_i=(x_{i1}, \dots, x_{im}) \in B^m$, $i=1, \dots, n$ set

$$w(x_1, \dots, x_n) = \big(p_1(x_{r(1)s(1)}), \dots, p_m(x_{r(m)s(m)})\big).$$

Now an algebra is a *wreath algebra* if it is isomorphic to an algebra on B^m with wreath operations only.

In [8] I. G. ROSENBERG gave a functional completeness criterion for finite algebras whose operations are all surjective. Among others he proved the following:

Theorem B (I. G. ROSENBERG [8]). *Let* $\mathbf{A}$ *be a finite algebra whose operations are all surjective.*

(i) *If* $\mathbf{A}$ *has a compatible at least binary central relation then it also has a compatible binary central relation.*

(ii) *If* $\mathbf{A}$ *has an operation depending on at least two variables,* $\mathbf{A}$ *is simple and has a compatible relation determined by an h-regular family of equivalence relations then it is a wreath algebra.*

An algebra (A, F) is said to be *affine* with respect to an elementary abelian group $(A; +)$ if it has a compatible relation of type (3) in Theorem A determined by $(A: +)$. To any finite field K and natural number n we associate the following affine algebra:

$$\mathbf{A}_{K,n} = \big(K^n;\, x-y+z,\, \{rx+(1-r)y\colon r \in K_{n\times n}\}\big)$$

where $K_{n\times n}$ is the $n \times n$ matrix ring over K.

Theorem C (Á. SZENDREI [10]). *Let* $\mathbf{A}$ *be an at least three element simple finite idempotent algebra. If* $\mathbf{A}$ *is affine with respect to an elementary abelian group then it is equivalent to* $\mathbf{A}_{K,n}$ *for some finite field* K *and* $n \geqq 1$.

2. Lemmas

Lemma 2.1. *An idempotent wreath algebra cannot be simple.*

Proof. Let B be a finite set with $|B|\geqq 3$, $m>1$, and consider an n-ary wreath operation w on B^m associated to permutations p_i of B ($i=1, \ldots, m$), and maps $r\colon M\to N$, $s\colon M\to M$ ($M=\{1, \ldots, m\}$, $N=\{1, \ldots, m\}$). It is easy to check that w is idempotent if and only if each p_i is the identity permutation on B, $i=1, \ldots, m$, and s is the identity permutation on M, i.e., for $x_i=(x_{i1}, \ldots, x_{im})\in B^m$, $i=1, \ldots, n$ we have

$$w(x_1, \ldots, x_n) = (x_{r(1)1}, \ldots, x_{r(m)m}).$$

Then w preserves the equivalence relations Θ_j ($j=1, \ldots, m$) defined by

$$\Theta_j = \{((a_1, \ldots, a_m), (b_1, \ldots, b_m))\in(B^m)^2\colon a_j = b_j\},$$

Lemma 2.2. *If an at least three element finite algebra with transitive automorphism groups has a compatible bounded partial order then it has a nontrivial compatible binary reflexive and symmetric relation.*

Proof. *Let* $\mathbf{A}=(A, F)$ be an at least three element finite algebra with transitive automorphism group and let ϱ be a compatible bounded partial order of $\mathbf{A}$ with least element 0 and greatest element 1. Choose an automorphism π of $\mathbf{A}$ with $1\pi\neq 0, 1$. Then the relation $\sigma=(\varrho\cap\varrho\pi)\circ(\varrho\cap\varrho\pi)^{-1}$, where $\varrho\pi=\{(x\pi, y\pi)\colon (x, y)\in\varrho\}$, is a compatible binary reflexive and symmetric relation of A. Furthermore, σ is nontrivial, since $(0, 1\pi)\in\varrho\cap\varrho\pi\subseteqq\sigma$ and $(1,1\pi)\notin\sigma$.

Lemma 2.3. *If an at least three element finite algebra has a nontrivial compatible binary reflexive and symmetric relation then it has either a nontrivial congruence relation, or a compatible at least binary central relation, or a compatible relation determined by an h-regular family of equivalence relations.*

Proof. Let $\mathbf{A}=(A, F)$ be an at least three element finite algebra and let σ be a nontrivial binary reflexive and symmetric relation on A with $(a, b)\in\sigma$, $a\neq b$. Suppose that σ is a compatible relation of $\mathbf{A}$, i.e. $F\subseteqq \mathrm{Pol}\,\sigma$. Since σ is nontrivial we have $\mathrm{Pol}\,\sigma\neq\mathbf{O}$. Therefore, by Theorem A, there is a relation ϱ of one of the types (1), ..., (6) such that $\mathrm{Pol}\,\sigma\subseteqq\mathrm{Pol}\,\varrho$. Clearly, ϱ is a compatible relation of $\mathbf{A}$. We have to show that ϱ is of type (4) or (6) or an at least binary relation of type (5). Since $\mathrm{Pol}\,\varrho$ contains all constant operations, it cannot be of type (2) or a unary central relation. Suppose that ϱ is a bounded partial order with least element 0 and greatest element 1. Consider the unary operations f and g defined by $f(0)=a$, $f(x)=b$ if $x\neq 0$ and $g(1)=a$, $g(x)=b$ if $x\neq 1$. Then $f, g\in\mathrm{Pol}\,\sigma\subseteqq\mathrm{Pol}\,\varrho$. Therefore $(a, b)=(f(0), f(1))\in\varrho$ and $(b, a)=(g(0), g(1))\in\varrho$, a contradiction. Finally suppose that ϱ is of type (3), and let $c \in A$ with $c \neq a, b$. Consider the unary operation h defined by $h(a)=a$ and $h(x)=b$ if $x \neq a$. Then $h \in \text{Pol}\, \varrho$, and $a+b-c \neq a$ as $c \neq a, b$. Therefore, $(a, b, c, a+b-c) \in \varrho$ implies $(a, b, b, b)=(h(a), h(b), h(c), h(a+b-c)) \in \varrho$, a contradiction.

3. Results and proofs

Theorem 3.1. *Let* **A** *be an at least three element finite idempotent algebra with transitive automorhism group. If* **A** *is simple and has no compatible binary central relation then it is either functionally complete or is equivalent to* $\mathbf{A}_{K,n}$ *for some finite field K and natural number n.*

Proof. Let **A** be a simple at least three element finite idempotent algebra with transitive automorphism group, and assume that A has no compatible binary central relation. If **A** is functionally incomplete then, by Theorem A, there is a relation ϱ of one of the types (1), ..., (6) such that Pol ϱ contains all algebraic functions of **A**. Since Pol ϱ contains all constant operations and **A** is simple, ϱ cannot be of type (2), (4) or a unary central relation. If ϱ is of type (6) then, by Theorem B, **A** is a wreath algebra and then, by Lemma 2.1, we have that **A** is not simple contrary to our assumption. If ϱ is an at least binary central relation then, again by Theorem B, **A** has a compatible binary central relation contrary to our assumption. Finally, if ϱ is a bounded partial order then taking into consideration Lemma 2.2 and 2.3, we obtain that **A** has a nontrivial congruence relation or an at least binary central relation or a compatible relation of type (6), which is a contradiction.

Hence ϱ is of type (3), i.e. A is affine with respect to an elementary abelian group and then, by Theorem C, we have that A is equivalent to $\mathbf{A}_{K,n}$ for some finite field K and $n \geqq 1$.

It is well-known (see e.g. [5] and [9]) that every nontrivial idempotent algebra has either a majority function or a Mal'tsev function or a nontrivial semi-projection or a nontrivial binary idempotent operation among its term functions.

Theorem 3.2. *If an at least there element finite idempotent algebra with transitive automorphism group is simple and has a majority function or a nontrivial semi-projection among its term functions then it is functionally complete.*

Proof. Let $\mathbf{A}=(A, F)$ be an at least three element simple finite idempotent algebra with transitive automorphism group that have a majority function or a nontrivial semi-projection among its term functions. It is well known (see e.g. [5] or [9]) that neither majority functions nor nontrivial semi-projections preserve a relation of type (3) and therefore **A** is not affine. Using Theorem 3.1, we have to show only that $\mathbf{A}$ has no compatible binary central relations. Suppose that $\mathbf{A}$ has a compatible binary central relation ϱ with center C and let $c\in C$.

First consider the case when $\mathbf{A}$ has an n-ary nontrivial semi-projection t among its term functions ($n\geqq 3$). We can suppose that t is a first semi-projection. We call a subset $I\subseteq A$ an ideal iff $t(a_1, \dots, a_n)\in I$ whenever $a_1\in I$. Since an intersection of ideals is an ideal again, we may speak about an ideal generated by a subset of A. For any $a\in A$ denote by $I(a)$ the ideal generated by $\{a\}$. Clearly, if I is an ideal and $\pi\in\operatorname{Aut}\mathbf{A}$ then $I\pi$ is again an ideal, and $I(a)\pi=I(a\pi)$. Because of the transitivity of Aut $\mathbf{A}$ the cardinalities of the 1-generated ideals are equal, and greater then one since t is not the first projection. So the 1-generated ideals form an Aut $\mathbf{A}$-invariant partition of A. Denote by θ the corresponding equivalence relation. Then θ is distinct from the identity relation and $\operatorname{Aut}\mathbf{A}\subseteq\operatorname{Pol}\theta$.

We show that $\theta\subseteq\varrho$, i.e. for any $a, b\in A$ we have $(a, b)\in\varrho$ if $I(a)=I(b)$. Let $a, b\in A$ with $I(a)=I(b)$. Consider the subset $I_a=\{x\colon (x, a)\in\varrho\}$. Then I_a is an ideal. Indeed, if $x_1\in I_a$ and $x_2,\dots, x_n\in A$ are arbitrary elements, then (x_1, a), $(x_2, c), \dots, (x_n, c)\in\varrho$ implies that $(t(x_1, \dots, x_n), a)=(t(x_1, x_2, \dots, x_n), t(a, c, \dots, c))\in\varrho$, i.e. $t(x_1, \dots, x_n)\in I_a$. Now, since I_a is an ideal with $a\in I_a$, we have $b\in I(b)=I(a)\subseteq I_a$ and $(b, a)\in\varrho$. Hence $\theta\subseteq\varrho$.

Consider the subalgebra σ of $\mathbf{A}^2$ generated by θ. Then $\theta\subseteq\sigma\subseteq\varrho$ and $F\cup\operatorname{Aut}\mathbf{A}\subseteq\operatorname{Pol}\sigma$, i.e., σ is a nontrivial compatible binary reflexive and symmetric relation of the algebra $\hat{\mathbf{A}}=(A; F\cup\operatorname{Aut}\mathbf{A})$. Taking into consideration Lemma 2.3, we have that $\hat{\mathbf{A}}$ has either a nontrivial congruence relation or an at least binary central relation or a relation of type (6). The first case cannot occur since $\hat{\mathbf{A}}$ is simple. In the third case, according to Theorem B, we obtain that $\hat{\mathbf{A}}$ and so $\mathbf{C}$ is a wreath algebra which, by Lemma 2.1, implies that $\mathbf{A}$ is not simple, a contradiction. In the second case let τ be an h-ary central relation of $\hat{\mathbf{A}}$, let u be an element in the center of τ, and let $a_1, \dots, a_h\in A$ be arbitrary elements. Choose a $\pi\in\operatorname{Aut}\mathbf{A}$ such that $u\pi=a_1$. Then $(u, a_2\pi^{-1}, \dots, a_h\pi^{-1})\in\tau$ implies that $(a_1, \dots, a_h)=(u\pi, (a_2\pi^{-1})\pi, \dots, (a_h\pi^{-1})\pi)\in\tau$. Hence τ is the full relation A^h, which is a contradicton. This completes the proof in the case when $\mathbf{A}$ has a nontrivial semi-projection among its term functions.

Now consider the case when $\mathbf{A}$ has a majority term function d. From now on we call a subset $I\subseteq A$ an ideal iff $d(x, y, z)\in I$ whenever at least two of the arguments belong to I. A and the one-element subsets are obviously ideals. Since an intersection of ideals is an ideal again, we may speak about an ideal generated by a subset of A. For any $a\in A$ the set $I_a=\{x|(x, a)\in\varrho\}$ is an ideal. Indeed, if for example $x, y\in I_a$ and $z\in A$ is arbitrary element, then $(x, a), (y, a), (z, z)\in\varrho$ implies that $(d(x, y, z), a)=(d(x, y, z), d(a, a, z))\in\varrho$, i.e. $d(x, y, z)\in I_a$. Clearly, if I is an ideal and $\pi\in\operatorname{Aut}\mathbf{A}$ then $I\pi$ is again an ideal.

Define a binary relation θ by setting $(a, b)\in\theta$ if and only if there is a minimal ideal (i.e. an ideal properly containing one-element ideals only) containing a and b. Then θ is distinct from the identity relation and $\mathrm{Aut}\, \mathbf{A} \subseteq \mathrm{Pol}\, \theta$. We show that $\theta \subseteq \varrho$. Indeed, let $(a, b) \in \theta$. If $a=b$ then $(a, b) \in \varrho$, too. If $a \neq b$ then put $u = d(a, b, c)$ (c is a central element of ϱ) and let I be the minimal ideal with $a, b \in I$. Now $a=d(a, b, a), b=d(a, b, b) \in I_u$. Since a and b are distinct, u is distinct from one of them, say $u \neq b$. By definition $u \in I$. We have $u, b \in I \cap I_b$, so by minimality of I, it follows that $I \subseteq I_b$, implying that $(a, b) \in \varrho$. Hence $\theta \subseteq \varrho$.

Consider the subalgebra σ of $\mathbf{A}^2$ generated by θ. Then $\theta \subseteq \sigma \subseteq \varrho$ and $F \cup \mathrm{Aut}\, \mathbf{A} \subseteq \mathrm{Pol}\, \sigma$, i.e., σ is a nontrivial compatible binary reflexive and symmetric relation of the algebra $\hat{\mathbf{A}} = (A; F \cup \mathrm{Aut}\, \mathbf{A})$. As we have seen above, this is impossible. This completes the proof in the case when A has a majority term function.

Theorem 3.3. *Every simple at least three element finite idempotent algebra with a Mal'tsev function among its term functions is either functionally complete or is equivalent to* $\mathbf{A}_{K,n}$ *for some finite K and natural number n.*

Proof. Let $\mathbf{A} = (A, F)$ be an at least three element simple finite idempotent algebra with a Mal'tsev function among its term functions. If $\mathbf{A}$ is functionally incomplete then, by the well-known Gumm—McKenzie Theorem (cf. e.g. in [2] and [3]) we have that $\mathbf{A}$ is affine. Finally apply Theorem C.

Problem. Is every at least three element finite simple idempotent algebra with transitive automorphism group either functionally complete or equivalent to $\mathbf{A}_{K,n}$ for some finite field K and natural number n?

As we have mentioned, every nontrivial idempotent algebra has either a majority function or a Mal'tsev function or a nontrivial semi-projection or a nontrivial binary idempotent operation among its term functions. Taking into consideration Theorem 3.2 and 3.3, the answer is positive if the algebra has either a majority function or a Mal'tsev function or a nontrivial semi-projection among its term functions. The remaining case is that, when the algebra has a nontrivial binary idempotent function and has neither a majority function nor a Mal'tsev function, nor a nontrivial semi-projection among its term functions.

References

[1] B. Csákány, Homogeneous algebras are functionally complete, *Algebra Universalis,* **11** (1980), 149—158.

[2] H. P. Gumm, Algebras in congruence permutable Varieties: Geometrical properties of affine algebras, *Algebra Universalis,* **9** (1979), 8—34.

[3] R. McKenzie, On minimal, locally finite varietis with permuting congruence relations, Preprint, 1976.

[4] P. P. Pálfy, L. Szabó and Á. Szendrei, Algebras with doubly transitive automorphism groups, in: *Finite Algebra and Multiple-Valued Logic* (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland (Amsterdam, 1981); pp. 521—535.

[5] P. P. Pálfy, L. Szabó and Á. Szendrei, Automorphism groups and functional completeness, *Algebra Universalis*, **15** (1982), 385—400.

[6] I. G. Rosenberg, Über die funktionale Vollständigkeit in den mehrwertigen Logiken (Struktur der Funktionen von mehreren Veränderlichen auf endlichen Mengen), *Rozpravy Československe Akad. Věd Řada Mat. Přirod. Věd*, **80** (1970), 9—93.

[7] I. G. Rosenberg, Completeness properties of multiple-valued logic algebras, in: *Computer Science and Multiple-Valued Logic, Theory and Applications* North-Holland Amsterdam, (1977); pp. 144—186.

[8] I. G. Rosenberg, Functional completeness of single generated or surjective algebras, in: *Finite Algebra and Multiple-Valued Logic* (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland (Amsterdam, 1981); pp. 635—652.

[9] L. Szabó and Á. Szendrei, Almost all algebras with triply transitive automorphism groups are functionally complete, *Acta Sci. Math.*, **41** (1979), 391—402.

[10] Á. Szendrei, *Clones in Universal Algebra*, Séminaire de Mathématiques Supérieures, vol. 99, Les Presses de l'Université de Montréal (Montréal, 1986).

BOLYAI INSTITUTE
ARADI VÉRTANÚK TERE 1
6720 SZEGED, HUNGARY