LINEAR EQUATIONAL THEORIES AND SEMIMODULE REPRESENTATIONS

Jaroslav Ježek and Tomáš Kepka

Abstract. Equational theories of some linear equations are studied. As a consequence, semimodule representations of the corresponding algebras are obtained. Examples are shown on medial and paramedial equations and some of their generalizations.

0. Introduction

For the classification of finite simple objects in a variety V of (universal) algebras, a crucial step may be to prove a representation theorem for V-algebras without irreducible elements. Consider, for example, the variety of medial groupoids. These are algebras with one binary, multiplicatively denoted operation satisfying $(xy)(zu) \approx (xz)(yu)$. A complete classification of finite simple medial groupoids was given in [4], and one of the crucial steps was to prove that for every medial groupoid G without irreducible elements there exists a commutative semigroup $S(+)$ with two commuting automorphisms f, g such that G is a subset of S and $ab = f(a) + g(b)$ for all $a, b \in G$.

We hope that a similar classification can be obtained for finite simple objects in some other varieties. The aim of this paper is to lay out equational and representational foundations for such results in a general setting. For varieties determined by an equation similar to the medial law, we can usually start by reducing the question to two special cases: that of simple finite zeropotent groupoids in the variety, and that of simple finite quasigroups in the variety. These two cases are then

1991 *Mathematics Subject Classification.* 08B05.

While working on this paper both authors were partially supported by the Grant Agency of Czech Republic, Grant No 201/96/0312.

handled separately: for the zeropotent case, the results of the present paper are essential, while in the second case different methods, specific to quasigroups, must be used. In papers [1], [2] and [3], the results of the present paper have been used to obtain the description of finite simple paramedial groupoids (groupoids satisfying $(xy)(zu) \approx (uy)(zx)$): the reduction to the two cases has been obtained, and all (not only finite) simple zeropotent paramedial groupoids have been completely described. (The quasigroup case has not yet been finished.)

Let V be a variety of algebras with one n-ary operation F, and let E denote the corresponding equational theory. We will suppose that E is based on a set of equations having the same variables at both sides and such that both sides are linear terms, i.e., terms in which every variable occurs at most once. The occurrences of variables in terms can be identified in a natural way with arbitrary words over the n-letter alphabet. With every linear equational theory E we can associate a congruence $\mathbf{C}_E$ of the free monoid over the n-letter alphabet, the congruence relating the two occurrences of any variable at both sides of any linear equation from E. On the other hand, with every congruence α of the free monoid we can associate a linear equational theory $\mathbf{E}_\alpha$, the largest equational theory such that $\mathbf{C}_{\mathbf{E}_\alpha} \subseteq \alpha$. This correspondence between linear equational theories and congruences of the free monoid is not one-to-one, but has some nice properties. It will be discussed in Section 2. The variety of models of $\mathbf{E}_{\mathbf{C}_E}$ is called the essential core of V. For example, the essential core of the variety of medial groupoids is the proper subvariety generated by medial cancellation groupoids; at the same time, it is just the variety generated by the medial groupoids having a representation in the above sense.

In the more general case, V-algebras will be represented by commutative semigroups $S(+)$ with an n-tuple of endomorphisms $h_1, \ldots, h_n$ satisfying equations induced by the congruence $\alpha = \mathbf{C}_E$. Such objects are called α-semimodules. In Section 4 we prove that every α-semimodule, considered as an algebra with one binary operation $h_1x_1 + \cdots + h_nx_n$, belongs to the essential core of V, and that free algebras in the essential core can be represented by α-semimodules. Consequently, the essential core of V is just the variety generated by the V-algebras having an α-semimodule representation. In Section 3 we formulate conditions under which every V-algebra without irreducible elements belongs to the essential core of V, and in

Section 5 conditions under which all such algebras have an α-semimodule representation. We also formulate conditions under which the free monoid can be replaced with the free group, and the endomorphisms of the representations are automorphisms. As an example, we show in Section 6 that all these conditions are satisfied for the variety of paramedial groupoids (groupoids satisfying $(xy)(zu) \approx (uy)(zx)$). For the variety of medial groupoids, the conditions are also satisfied.

In the trivial case of the variety of all algebras (with one n-ary operation F, $n \geq 2$) the conditions are also satisfied. It follows that for any algebra $A(F)$ there exists a commutative semigroup $S(+)$ and an n-tuple $h_1, \ldots, h_n$ of automorphisms of $S(+)$ such that A is a subset of S and $F(a_1, \ldots, a_n) = h_1(a_1) + \cdots + h_n a_n$ for all $a_1, \ldots, a_n \in A$. However, this result is not as deep as in the case of varieties satisfying particular equations, and does not seem to have applications.

1. Linear equational theories

For the basics of universal algebra and equational logic, the reader is referred to [7].

Let $n \geq 2$ be an integer. Let us take one fixed operation symbol F of arity n. Unless specified otherwise, all our algebras, terms, equational theories, etc., will be of the signature consisting of this single operation symbol. The fundamental operation of an algebra A will be denoted by F_A. By a term we mean an element of the absolutely free algebra over the infinite countable set X of variables. The algebra of terms will be denoted by T. By a substitution we mean an endomorphism of T. A substitution is called short if it maps the set X into itself.

We fix n different symbols $F_1, \ldots, F_n$ and denote by M the free monoid over the set $\{F_1, \ldots, F_n\}$; its elements are called words. The empty word is the unit of M; it will be denoted by $\emptyset$. A word f is said to be a subword of a word e if $e = gfh$ for some words g and h. Two words e and f are called comparable if either e is a beginning of f or f is a beginning of e. In all other cases, the two words are incomparable. The length of a word e is denoted by $|e|$.

The elements of M can be used to represent the nodes of the rooted n-ary tree, corresponding to a given term t. For a given term t, we denote by $\mathcal{O}(t)$ the (finite) subset of M consisting of the nodes of the tree of t, and for each $e \in \mathcal{O}(t)$ we denote by $t[e]$ the corresponding subterm of t. More precisely, we can define $\mathcal{O}(t)$

and $t[e]$ (for $e \in \mathcal{O}(t)$) by induction on the complexity of t as follows: If $t \in X$, then $\mathcal{O}(t) = \{\emptyset\}$; $t[\emptyset] = t$. If $t = Ft_1 \dots t_n$, then $\mathcal{O}(t) = \{\emptyset\} \cup \bigcup_{i=1}^{n} \{F_i e : e \in \mathcal{O}(t_i)\}$; $t[\emptyset] = t$ and $t[F_i e] = t_i[e]$.

The elements of $\mathcal{O}(t)$ are called occurrences in t. If $e \in \mathcal{O}(t)$ and $t[e] = w$, we say that e is an occurrence of a subterm w in t. We denote by $\mathcal{O}_X(t)$ the (finite) set of occurrences of variables in t. The set of variables occurring in t will be denoted by $\mathbf{S}(t)$ and called the support of t. A term t is called linear if every variable has at most one occurrence in t. Two terms u and v are called similar if $v = \varphi(u)$ for an automorphism φ of T, i.e., if $\mathcal{O}_X(u) = \mathcal{O}_X(v)$ and whenever $e, f \in \mathcal{O}_X(u)$, then $u[e] = u[f]$ if and only if $v[e] = v[f]$.

Let t be a term and e, f be two incomparable words from $\mathcal{O}(t)$. We denote by $t^{(e,f)}$ the (unique) term such that $t^{(e,f)}[e] = t[f]$, $t^{(e,f)}[f] = t[e]$ and $t^{(e,f)}[g] = t[g]$ for all $g \in \mathcal{O}_X(t)$ incomparable with both e and f. If $e, f \in \mathcal{O}_X(t)$, then $\mathcal{O}_X(t) = \mathcal{O}_X(t^{(e,f)})$.

By an isosceles term of depth k we mean a term t such that $|e| = k$ for any $e \in \mathcal{O}_X(t)$. Equivalently: A term t is an isosceles term of depth k if and only if $\mathcal{O}_X(t)$ is the set of all words of length k.

By an equation we mean an ordered pair $\langle u, v\rangle$ of terms; we will sometimes write $u \approx v$ instead of $\langle u, v\rangle$. By an equational theory we mean a fully invariant congruence of the term algebra.

An equation $u \approx v$ is called regular if $\mathbf{S}(u) = \mathbf{S}(v)$. An equation $u \approx v$ is called balanced if every variable has the same number of occurrences in u as in v. An equation $u \approx v$ is called linear if it is regular and both u and v are linear terms. While the set of regular equations, as well as the set of balanced equations, are equational theories, the same is not true for linear equations. An equational theory is called linear if it is based on a set of linear equations. Every linear equational theory is balanced, and every balanced equational theory is regular.

1.1. Theorem. *Let E be a linear equational theory. Then for any equation $\langle u, v\rangle \in E$ there exists a linear equation $\langle u', v'\rangle \in E$ such that $\sigma(u') = u$ and $\sigma(v') = v$ for a short substitution σ.*

Proof. Denote by E' the set of the equations $\langle u, v\rangle \in E$ for which such a linear equation $\langle u', v'\rangle$ exists. Let B be a base for E, consisting of linear equations.

Clearly, B is contained in E' and so it remains to prove that E' is an equational theory.

The reflexivity and symmetry of E' are obvious. Let us prove the transitivity. Let $\langle u, v\rangle \in E'$ and $\langle v, w\rangle \in E'$. There exist linear equations $\langle u', v'\rangle \in E$, $\langle v'', w''\rangle \in E$ and short substitutions σ_1, σ_2 with $u = \sigma_1(u')$, $v = \sigma_1(v') = \sigma_2(v'')$ and $w = \sigma_2(w'')$. Since the terms v' and v'' are linear and have a common short substitution instance, they are similar. There exists an automorphism φ of T with $v'' = \varphi(v')$. Since $\sigma_1(v') = v = \sigma_2\varphi(v')$, we have $\sigma_1(x) = \sigma_2\varphi(x)$ for every $x \in \mathbf{S}(v') = \mathbf{S}(u')$, and hence $u = \sigma_1(u') = \sigma_2\varphi(u')$. We get $\langle u, w\rangle \in E'$, since $\langle \varphi(u'), v''\rangle$ is a linear equation belonging to E (because $\varphi(u')\ E\ \varphi(v') = v''\ E\ w''$) and σ_2 is a short substitution with $u = \sigma_2\varphi(u')$ and $w = \sigma_2(w'')$.

It is easy to see that E' is a congruence. So it remains to prove that $\langle u, v\rangle \in E'$ implies $\langle \varphi(u), \varphi(v)\rangle \in E'$ for any substitution φ. There exist a linear equation $\langle u', v'\rangle \in E$ and a short substitution σ with $u = \sigma(u')$ and $v = \sigma(v')$. For every $x \in \mathbf{S}(u') = \mathbf{S}(v')$ take a linear term $\psi(x)$ similar with $\varphi\sigma(x)$, in such a way that the supports of the terms $\psi(x)$ are pairwise disjoint for different variables x. Because of this disjointness, there exists a short substitution κ such that $\kappa\psi(x) = \varphi\sigma(x)$ for all $x \in \mathbf{S}(u') = \mathbf{S}(v')$. Hence $\kappa\psi(u') = \varphi\sigma(u') = \varphi(u)$ and $\kappa\psi(v') = \varphi(v)$. Since $\langle \psi(u'), \psi(v')\rangle$ is a linear equation belonging to E, we get $\langle \varphi(u), \varphi(v)\rangle \in E'$. □

2. The correspondence

Let α be a congruence of M. We define a binary relation $\mathbf{E}_\alpha$ on T as follows: $u\ \mathbf{E}_\alpha\ v$ if and only if there exists a bijection h of $\mathcal{O}_X(u)$ onto $\mathcal{O}_X(v)$ such that $u[e] = v[h(e)]$ and $e\ \alpha\ h(e)$ for all $e \in \mathcal{O}_X(u)$. (Such a bijection h will be called α-admissible for u, v.)

Let E be an equational theory. We define a binary relation $\mathbf{C}_E$ on M by $e\ \mathbf{C}_E\ f$ if and only if there exists a linear equation $\langle u, v\rangle \in E$ such that $e \in \mathcal{O}_X(u)$, $f \in \mathcal{O}_X(v)$ and $u[e] = v[f]$.

2.1. Theorem.

(1) *If α is a congruence of M, then $\mathbf{E}_\alpha$ is a linear equational theory.*

(2) *If E is a linear equational theory, then $\mathbf{C}_E$ is a congruence of M.*

(3) *$\alpha_1 \subseteq \alpha_2$ implies $\mathbf{E}_{\alpha_1} \subseteq \mathbf{E}_{\alpha_2}$ for any pair of congruences α_1, α_2 of M.*

(4) $E_1 \subseteq E_2$ *implies* $\mathbf{C}_{E_1} \subseteq \mathbf{C}_{E_2}$ *for any pair of linear equational theories* E_1, E_2.

(5) $\mathbf{C}_{\mathbf{E}_\alpha} \subseteq \alpha$ *for any congruence* α *of* M.

(6) $E \subseteq \mathbf{E}_{\mathbf{C}_E}$ *for any linear equational theory* E.

Proof. (1) The relation $\mathbf{E}_\alpha$ is an equivalence, since α is an equivalence. It is a congruence of T, since α is a left congruence of M (i.e., $e\ \alpha\ f$ implies $F_i e\ \alpha\ F_i f$ for any $i \in \{1, \dots, n\}$). Let $u\ \mathbf{E}_\alpha\ v$ and let φ be a substitution. There exists an α-admissible bijection h for u, v. If $e \in \mathcal{O}_X(\varphi(u))$, then e can be uniquely decomposed into $e = e_1 e_2$ where $e_1 \in \mathcal{O}_X(u)$; define $g(e) = h(e_1)e_2$. It is easy to see that g is a bijection of $\mathcal{O}_X(\varphi(u))$ onto $\mathcal{O}_X(\varphi(v))$ and $\varphi(u)[e] = \varphi(v)[g(e)]$. We have $e\ \alpha\ g(e)$, since $e_1\ \alpha\ h(e_1)$ implies $e_1 e_2\ \alpha\ h(e_1)e_2$. So, g is α-admissible for $\varphi(u), \varphi(v)$ and $\mathbf{E}_\alpha$ is an equational theory.

Let $\langle u, v\rangle \in \mathbf{E}_\alpha$ and let h be an α-admissible bijection for u, v. Clearly, there is a linear term u' with $\mathcal{O}_X(u') = \mathcal{O}_X(u)$. There is a unique term v' with $\mathcal{O}_X(v') = \mathcal{O}_X(v)$ and $v'[e] = u'[h^{-1}(e)]$ for all $e \in \mathcal{O}_X(v')$. It is easy to check that $\langle u', v'\rangle \in \mathbf{E}_\alpha$, $\langle u', v'\rangle$ is a linear equation and $\langle u, v\rangle$ is a consequence of $\langle u', v'\rangle$. This shows that $\mathbf{E}_\alpha$ is a linear equational theory.

(2) The reflexivity and symmetry of $\mathbf{C}_E$ are clear. In order to prove transitivity, let $e\ \mathbf{C}_E\ f\ \mathbf{C}_E\ g$. There are linear equations $\langle u, v_1\rangle \in E$ and $\langle v_2, w\rangle \in E$ with $e \in \mathcal{O}_X(u)$, $f \in \mathcal{O}_X(v_1) \cap \mathcal{O}_X(v_2)$, $g \in \mathcal{O}_X(w)$, $u[e] = v_1[f]$ and $v_2[f] = w[g]$. Clearly, there is a linear term v such that $f \in \mathcal{O}_X(v)$, $\mathcal{O}_X(v_1) \subseteq \mathcal{O}(v)$ and $\mathcal{O}_X(v_2) \subseteq \mathcal{O}(v)$. There are substitutions σ_1 and σ_2 with $v = \sigma_1(v_1) = \sigma_2(v_2)$. We have $\langle \sigma_1(u), \sigma_1(v_1)\rangle \in E$ and $\langle \sigma_2(v_2), \sigma_2(w)\rangle \in E$. Since $\sigma_1(v_1) = \sigma_2(v_2)$, we get $\langle \sigma_1(u), \sigma_2(w)\rangle \in E$. Clearly, this is a linear equation. Since

$$\sigma_1(u)[e] = \sigma_1(u[e]) = \sigma_1(v_1[f]) = v[f] = \sigma_2(v_2[f]) = \sigma_2(w[g]) = \sigma_2(w)[g],$$

we get $e\ \mathbf{C}_E\ g$. This shows that $\mathbf{C}_E$ is an equivalence. It is a left congruence, since E is a congruence; it is a right congruence, since E is fully invariant.

(3) and (4) are evident, and (5) is easy. Let us prove (6). Since E is a linear equational theory, it is sufficient to show that every linear equation $\langle u, v\rangle \in E$ belongs to $\mathbf{E}_{\mathbf{C}_E}$. There is a unique bijection h of $\mathcal{O}_X(u)$ onto $\mathcal{O}_X(v)$ with $u[e] = v[h(e)]$ for all $e \in \mathcal{O}_X(u)$. We have $e\ \mathbf{C}_E\ h(e)$ for any $e \in \mathcal{O}_X(u)$ by definition, and hence $\langle u, v\rangle \in \mathbf{E}_{\mathbf{C}_E}$. $\square$

Let us call an equational theory E essential if $E = \mathbf{E}_\alpha$ for a congruence α of M. Of course, every essential equational theory is linear. Let us call a congruence α of M essential if $\alpha = \mathbf{C}_E$ for a linear equational theory E.

2.2. Theorem. *A linear equational theory E is essential if and only if it contains any linear equation $\langle u, v\rangle$ such that for any e, f with $u[e] = v[f]$ there exists a linear equation $\langle u', v'\rangle \in E$ with $u'[e] = v'[f]$.*

$\alpha \mapsto \mathbf{E}_\alpha$ is an isomorphism of the complete lattice of essential congruences of M onto the complete lattice of essential equational theories, and $E \mapsto \mathbf{C}_E$ is the inverse isomorphism.

Proof. By (3), (5) and (6) of Theorem 2.1, $\mathbf{E}_{\mathbf{C}_E} = E$ if $E = \mathbf{E}_\alpha$ for some α, i.e., if E is essential. Similarly, $\mathbf{C}_{\mathbf{E}_\alpha} = \alpha$ whenever α is essential. From this it follows that the two mappings are mutually inverse, order preserving bijections between the set of essential equational theories and the set of essential congruences. A linear equational theory E is essential iff $\mathbf{E}_{\mathbf{C}_E} = E$ iff $\mathbf{E}_{\mathbf{C}_E} \subseteq E$ iff every linear equation from $\mathbf{E}_{\mathbf{C}_E}$ belongs to E, and this condition can be reformulated according to the definitions. From this characterization it follows easily that the intersection of an arbitrary collection of essential equational theories is again essential, so that the set of essential equational theories is a complete lattice (with respect to inclusion). □

For a given linear equational theory E, the equational theory $\mathbf{E}_{\mathbf{C}_E}$ will be called the essential closure of E. It is just the least essential equational theory containing E.

It is easy to see that for any pair e, f of words there exists a term t such that $e, f \in \mathcal{O}_X(t)$ and whenever $e, f \in \mathcal{O}_X(t')$ for some t', then t' is a substitution instance of t; this term t is linear and is uniquely determined up to similarity. It will be denoted by $J_{e,f}$. (More precisely, we take one fixed term in the similarity class of u and denote it by $J_{e,f}$.) Let e, f be two incomparable words. Recall that, according to the above definitions, $J_{e,f}^{(e,f)}$ is the term obtained from $J_{e,f}$ by transposing the variables at e and f.

2.3. Lemma. *Let e, f be two incomparable words. Then for a congruence α of M, $e\ \alpha\ f$ if and only if $\langle J_{e,f}, J_{e,f}^{(e,f)}\rangle \in \mathbf{E}_\alpha$.*

Proof. It is easy. □

A congruence α of M is said to be length preserving if $e\ \alpha\ f$ implies $|e| = |f|$.

2.4. Theorem. *Every length preserving congruence of M is essential. More generally, if α is a congruence of M such that e, f are incomparable whenever $e\ \alpha\ f$ and $e \neq f$, then α is essential.*

Proof. It follows from Lemma 2.3. □

2.5. Theorem. *Let E be a linear equational theory and B be a base for E consisting of linear equations. Denote by α_0 the set of the ordered pairs $\langle e, f\rangle$ such that there is an equation $\langle u, v\rangle \in B$ with $e \in \mathcal{O}_X(u)$, $f \in \mathcal{O}_X(v)$ and $u[e] = v[f]$. Then $\mathbf{C}_E$ is the congruence of M generated by α_0.*

Consequently, if E is a finitely based linear equational theory, then $\mathbf{C}_E$ is a finitely generated congruence of M.

Proof. Denote by α the congruence generated by α_0. Clearly, $\alpha \subseteq \mathbf{C}_E$. Let $\langle e, f\rangle \in \mathbf{C}_E$, so that $u[e] = v[f]$ for some linear equation $\langle u, v\rangle \in E$. There exists a derivation of $\langle u, v\rangle$ based on B, i.e., a finite sequence $p_0, \dots, p_k$ of terms such that $u = p_0$, $v = p_k$ and every p_{i+1} is obtained from p_i by replacing a subterm $p_i[g_i] = \sigma_i(u_i)$ with $\sigma_i(v_i)$ for some $g_i \in \mathcal{O}_X(p_i)$, some equation $\langle u_i, v_i\rangle \in B \cup B^{-1}$ and some substitution σ_i. Let us define a word $e_i \in \mathcal{O}_X(p_i)$ by induction on i as follows: $e_0 = e$; e_{i+1} is the only word from $\mathcal{O}_X(p_{i+1})$ with $p_i[e_i] = p_{i+1}[e_{i+1}]$. Clearly, $e_k = f$. In order to prove $\langle e, f\rangle \in \alpha$, it is sufficient to prove $\langle e_i, e_{i+1}\rangle \in \alpha$ for all $i = 0, \dots, k-1$. If e_i is incomparable with g_i, then $e_{i+1} = e_i$. So, let e_i be comparable with g_i. We have $e_i = g_i rs$ for some $r \in \mathcal{O}_X(u_i)$ and $s \in \mathcal{O}_X(\sigma_i(u_i[r]))$. Put $x = u_i[r]$ and $y = \sigma_i(x)[s]$. There is a unique word $r' \in \mathcal{O}_X(v_i)$ with $v_i[r'] = x$; we have $\langle r, r'\rangle \in \alpha_0$ by definition. It is easy to see that $p_{i+1}[g_i r's] = y = p_i[g_i rs] = p_i[e_i]$, and hence $e_{i+1} = g_i r's$. Since $\langle r, r'\rangle \in \alpha$, we get $\langle g_i rs, g_i r's\rangle \in \alpha$, i.e., $\langle e_i, e_{i+1}\rangle \in \alpha$. □

An equational theory E is called cancellative if $\langle Fu_1 \dots u_n, Fv_1 \dots v_n\rangle \in E$ and $i \in \{1, \dots, n\}$ imply $\langle u_i, v_i\rangle \in E$ whenever $u_j = v_j$ for all $j \neq i$. A congruence α of M is called left cancellative if $ef\ \alpha\ eg$ implies $f\ \alpha\ g$.

2.6. Theorem. *If α is a left cancellative congruence of M, then $\mathbf{E}_\alpha$ is cancellative. If E is a cancellative linear equational theory, then $\mathbf{C}_E$ is left cancellative.*

Proof. It is easy. □

The variety of models of $\mathbf{E}_\alpha$ will be denoted by $\mathbf{V}_\alpha$. A variety is called linear if the corresponding equational theory is linear. A variety is called essential if the corresponding equational theory is essential. If V is a linear variety, then the largest essential variety contained in V will be called the essential core of V; it is the variety of models of the essential closure of the equational theory of V.

It has been proved in [4] that the essential core of the variety of medial groupoids is just the variety generated by medial cancellation groupoids. A similar result has been proved for paramedial groupoids (these are groupoids satisfying $(xy)(zu) \approx (uy)(zx)$) in [6]. We do not know, however, if the two results have an elegant common generalization.

As it is easy to see, every finitely based linear (or, more generally, balanced) equational theory E is decidable. The essential closure of E is a linear equational theory which is not, however, finitely based in many cases. For example, the essential closure of the equational theory of medial groupoids is not finitely based. This has been proved in [4]; more strongly, Pollák and Szendrei [8] prove that the essential closure has an infinite, independent base. In spite of this fact, the essential closures are decidable equational theories in many cases:

2.7. Theorem. *Let E be a finitely based linear equational theory such that $\mathbf{C}_E$ is a length preserving congruence of M. Then the essential closure of E is a decidable equational theory.*

Proof. By 2.5, $\mathbf{C}_E$ is a finitely generated congruence. It is easy to see that every finitely generated, length preserving congruence of M is decidable and, by the definition of $\mathbf{E}_\alpha$, the equational theory $\mathbf{E}_\alpha$ is decidable whenever α is a decidable congruence. □

On the other hand, we do not know if the class of finite models of the essential closure of a finitely based linear equational theory is always recursive. We do not know it even in very simple particular cases. The following open problem can be pointed out: Is the class of finite groupoids from the essential core of the variety of medial groupoids recursive?

3. Algebras without irreducible elements

An element a of an algebra A (of signature $\{F\}$) is called irreducible if there is

no n-tuple $b_1, \dots, b_n$ with $a = F_A(b_1, \dots, b_n)$.

Let e, f be a pair of words with $|e| = |f|$ and $e \neq f$. A linear equation $\langle u, v\rangle$ is said to be (e, f)-separating if $e, f \in \mathcal{O}_X(u) = \mathcal{O}_X(v)$, $u[e] = v[f]$, $u[f] = v[e]$ and $u[g] = v[g]$ for all $g \in \mathcal{O}_X(u) - \{e, f\}$. We call an equation $\langle u, v\rangle$ separating if it is (e, f)-separating for some e, f.

A linear equational theory E is said to be separable if $\mathbf{C}_E$ is a length preserving congruence of M and for any $\langle e, f\rangle \in \mathbf{C}_E$ with $e \neq f$ there exists an (e, f)-separating equation $\langle u, v\rangle \in E$. A linear variety is said to be separable if its equational theory is separable.

3.1. Theorem. *Let V be a separable linear variety. Then every algebra from V without irreducible elements belongs to the essential core of V.*

Proof. Denote by E the equational theory of V and by E' the essential closure of E (so that E' is the equational theory of the essential core of V). Let $A \in V$ be an algebra without irreducible elements. We need to prove that every linear equation $\langle u, v\rangle \in E'$ is satisfied in A.

Let $\langle e, f\rangle \in \mathbf{C}_E$ and put $k = |e| = |f|$. For every term t with $e, f \in \mathcal{O}_X(t)$ denote by t' the term such that $\mathcal{O}_X(t') = \mathcal{O}_X(t)$, $t'[e] = t[f]$, $t'[f] = t[e]$ and $t'[g] = t[g]$ for all $g \in \mathcal{O}_X(t) - \{e, f\}$. Let us call a term t admissible if it is linear, $e, f \in \mathcal{O}_X(t)$ and $\langle t, t'\rangle$ is satisfied in A. Since E is separable, there exists at least one admissible term. An application of a suitable substitution provides us with an admissible term t such that $|g| \geq k$ for all $g \in \mathcal{O}_X(t)$. Suppose that there is a word $g \in \mathcal{O}_X(t)$ of length at least k, such that $t[g] = F(x_1, \dots, x_n)$ for some (pairwise distinct) variables $x_1, \dots, x_n$. Of course, g is incomparable with both e and f. Denote by w the term obtained from t by replacing the subterm at g with a variable not belonging to t. Since A is an algebra without irreducible elements and $\langle t, t'\rangle$ is satisfied in A, it is easy to see that also $\langle w, w'\rangle$ is satisfied in A; hence w is also admissible. In this way we can replace any admissible, non-isosceles term t such that $|g| \geq k$ for all $g \in \mathcal{O}_X(t)$, with a new term w which is closer to an isosceles term of depth k and satisfies the same condition. Consequently, there exists an isosceles admissible term of depth k.

Let t be an isosceles term of depth k. For every permutation p of $\mathcal{O}_X(t)$ denote by t^p the term with $\mathcal{O}_X(t^p) = \mathcal{O}_X(t)$ and $t^p[e] = t[p(e)]$ for all $e \in \mathcal{O}_X(t)$. Denote

by P the group of the permutations p for which $\langle t, t^p \rangle$ is satisfied in A. We have seen that every transposition (e, f) with $\langle e, f \rangle \in \mathbf{C}_E$ belongs to P. Now every permutation p with the property $\langle e, p(e) \rangle \in \mathbf{C}_E$ for all words e of length k can be expressed as the product of such transpositions, and consequently belongs to P.

This shows that the algebra A satisfies any linear equation $\langle p, q \rangle \in E'$ such that p is an isosceles term. If $\langle u, v \rangle$ is any linear equation from E', then for a suitable substitution σ, the term $\sigma(u)$ is a linear isosceles term. The equation $\langle \sigma(u), \sigma(v) \rangle$ is satisfied in A. Since A is an algebra without irreducible elements, it follows that $\langle u, v \rangle$ is satisfied in A. $\square$

Given an equational theory E, we denote by $\mathbf{C}_E^0$ the set of the ordered pairs $\langle e, f \rangle$ of words such that $|e| = |f|$ and $\langle t, t^{(e,f)} \rangle \in E$ for any linear isosceles term t of depth $|e|$.

3.2. Lemma. *Let E be a linear equational theory. Then $\mathbf{C}_E^0$ is a left congruence of M and $\mathbf{C}_E^0 \subseteq \mathbf{C}_E$. If $\mathbf{C}_E^0 = \mathbf{C}_E$, then E is separable.*

Proof. It is easy. $\square$

3.3. Theorem. *Let E be a linear equational theory such that the following conditions are satisfied:*

(1) *$\mathbf{C}_E$ is a cancellative, length preserving congruence;*
(2) *if $\langle F_i e F_k, F_j f F_l \rangle \in \mathbf{C}_E$ where $i \neq j$, then either $\langle F_i e F_k, F_j f F_l \rangle \in \mathbf{C}_E^0$ or $\langle e F_k, g \rangle \in \mathbf{C}_E$ for some g incomparable with e or $\langle f F_l, g \rangle \in \mathbf{C}_E$ for some g incomparable with f;*
(3) *if $\langle F_i e F_k, F_j f F_l \rangle \in \mathbf{C}_E$ where $i \neq j$, then either $\langle F_i e F_k, F_j f F_l \rangle \in \mathbf{C}_E^0$ or $\langle e F_k, g F_l \rangle \in \mathbf{C}_E$ for some g or $\langle f F_l, g F_k \rangle \in \mathbf{C}_E$ for some g.*

Then E is separable.

Proof. By 3.2 it is enough to prove $\mathbf{C}_E \subseteq \mathbf{C}_E^0$. Let us prove by induction on $|e|$ that $\langle e, f \rangle \in \mathbf{C}_E$ implies $\langle e, f \rangle \in \mathbf{C}_E^0$. If $|e| \leq 1$, it is clear. Let $e = F_i e_0 F_k$ and $f = F_j f_0 F_l$.

If $i = j$, then $\langle e_0 F_k, f_0 F_l \rangle \in \mathbf{C}_E$ by left cancellation, so that $\langle e_0 F_k, f_0 F_l \rangle \in \mathbf{C}_E^0$ by the induction assumption and hence $\langle e, f \rangle = \langle F_i e_0 F_k, F_i f_0 F_l \rangle \in \mathbf{C}_E^0$.

Let $i \neq j$. Consider first the case $k = l$. By right cancellation, $\langle F_i e_0, F_j f_0 \rangle \in \mathbf{C}_E$; by induction, $\langle F_i e_0, F_j f_0 \rangle \in \mathbf{C}_E^0$. By (2), without loss of generality $\langle e_0 F_k, g \rangle \in \mathbf{C}_E$

for some g incomparable with e_0. By induction, $\langle e_0F_k, g\rangle \in \mathbf{C}_E^0$. Consequently, $\langle e, F_ig\rangle \in \mathbf{C}_E^0$. Let t be an isosceles term of depth $|e|$. Put

$$t' = t^{(e,F_ig)(F_ie_0,F_jf_0)(e,F_ig)(F_ie_0,F_jf_0)(e,F_ig)},$$

so that $\langle t, t'\rangle \in E$ by the definition of $\mathbf{C}_E^0$. It is easy to check that $t' = t^{(e,f)}$. Consequently, $\langle t, t^{(e,f)}\rangle \in E$ and $\langle e, f\rangle \in \mathbf{C}_E^0$.

Now let $k \neq l$. By (3), without loss of generality $\langle e_0F_k, gF_l\rangle \in \mathbf{C}_E$ for some g. By induction, $\langle e_0F_k, gF_l\rangle \in \mathbf{C}_E^0$. Consequently, $\langle F_ie_0F_k, F_igF_l\rangle \in \mathbf{C}_E^0$. Since $\langle F_jf_0F_l, F_igF_l\rangle \in \mathbf{C}_E$, it follows from the previous step of the proof that the ordered pair $\langle F_jf_0F_l, F_igF_l\rangle$ belongs to $\mathbf{C}_E^0$. We get $\langle e, f\rangle \in \mathbf{C}_E^0$ by transitivity. □

3.4. Corollary. *Let E be a linear equational theory having a base B such that every equation from B is (e, f)-separating for some e, f and the following conditions are satisfied:*

(1) $\mathbf{C}_E$ *is a cancellative, length preserving congruence;*

(2) *if $\langle F_ieF_k, F_jfF_l\rangle \in \mathbf{C}_E - (B \cup B^{-1})$ where $i \neq j$, then either $\langle eF_k, g\rangle \in \mathbf{C}_E$ for some g incomparable with e or $\langle fF_l, g\rangle \in \mathbf{C}_E$ for some g incomparable with f;*

(3) *if $\langle F_ieF_k, F_jfF_l\rangle \in \mathbf{C}_E - (B \cup B^{-1})$ where $i \neq j$, then either $\langle eF_k, gF_l\rangle \in \mathbf{C}_E$ for some g or $\langle fF_l, gF_k\rangle \in \mathbf{C}_E$ for some g.*

Then E is separable. □

4. Free algebras

Let α be a congruence of M. By an α-semimodule we mean a universal algebra of the signature $\{+, 0, F_1, \ldots, F_n\}$ where $+$ is a binary operation symbol, 0 is a constant, F_i are considered as unary operation symbols and the following identities are satisfied:

$$(x + y) + z \approx x + (y + z),$$

$$x + y \approx y + x,$$

$$x + 0 \approx x,$$

$$F_i(x + y) \approx F_ix + F_iy \quad (i = 1, \ldots, n),$$

$$F_i0 \approx 0 \quad (i = 1, \ldots, n),$$

$$ex \approx fx \quad \text{for any } \langle e, f\rangle \in \alpha.$$

Clearly, the class of α-semimodules is a variety. It is easy to see that the infinite collection of identities $ex \approx fx$ can be equivalently replaced by $\{ex \approx fx : \langle e, f\rangle \in K\}$ for any generating subset K of α. Consequently, the variety of α-semimodules is finitely based whenever α is a finitely generated congruence of M.

Let S be an α-semimodule. We can define an n-ary operation F_S on S by

$$F_S(a_1, \dots, a_n) = F_1 a_1 + \cdots + F_n a_n.$$

In this way, every α-semimodule becomes an algebra (of signature $\{F\}$).

4.1. Theorem. *Let α be a congruence of M and S be an α-semimodule.*

(1) *For a homomorphism φ of the term algebra T (of signature $\{F\}$) into S and for a term t,*

$$\varphi(t) = \sum_{e \in \mathcal{O}_X(t)} e\varphi(t[e]).$$

(2) *The algebra S, considered as an algebra of signature $\{F\}$, belongs to $\mathbf{V}_\alpha$.*

Proof. (1) is easy by induction on the complexity of t. In order to prove (2), let φ be a homomorphism of T into S and let $\langle u, v\rangle \in \mathbf{E}_\alpha$. There is a bijection h of $\mathcal{O}_X(u)$ onto $\mathcal{O}_X(v)$ such that $u[e] = v[h(e)]$ and $e \ \alpha \ h(e)$ for all $e \in \mathcal{O}_X(u)$. It follows easily from (1) that $h(u) = h(v)$. $\square$

Let Y be a nonempty set. The free α-semimodule over Y will be denoted by H_Y^α. Clearly, its elements can be expressed in the form $\sum_{i=1}^r e_i y_i$ where $r \geq 0$, $y_i \in Y$ and $e_i \in M$; we have $\sum_{i=1}^r e_i y_i = \sum_{j=1}^s f_j z_j$ if and only if $r = s$ and there is a permutation h of $\{1, \dots, r\}$ such that $y_i = z_{h(i)}$ and $e_i \ \alpha \ f_{h(i)}$ for all i.

The $\{F\}$-subalgebra of H_Y^α generated by Y will be denoted by G_Y^α.

4.2. Theorem. *Let α be a congruence of M and Y be a nonempty set. Then G_Y^α is the free algebra in the variety $\mathbf{V}_\alpha$ over Y. An element $e_1 y_1 + \dots e_k y_k$ of H_Y^α belongs to G_Y^α if and only if $k > 0$ and there exist pairwise incomparable words $f_1 \ \alpha \ e_1, \dots, f_k \ \alpha \ e_k$ such that whenever $f_i = ef$ for some words e and f, where f is nonempty, then for every $j \in \{1, \dots, n\}$ there exists an i' with $f_{i'} = eF_j g$ for some word g.*

Proof. Consider first the case $Y = X$. Denote by φ the homomorphism of T onto G_X^α extending the identity on X. For two terms u and v we have $\varphi(u) =$

$\sum_{e\in\mathcal{O}_X(u)} eu[e]$ and $\varphi(v)=\sum_{f\in\mathcal{O}_X(v)} fv[f]$, so $\varphi(u)=\varphi(v)$ if and only if there is a bijection h of $\mathcal{O}_X(u)$ onto $\mathcal{O}_X(v)$ such that $u[e]=v[h(e)]$ and $e\ \alpha\ h(e)$ for all $e\in\mathcal{O}_X(u)$, i.e., if and only if $\langle u,v\rangle\in\mathbf{E}_\alpha$. Hence G_X^α is isomorphic to the factor of T by $\mathbf{E}_\alpha$, which is a free algebra in the variety $\mathbf{V}_\alpha$.

The general case follows easily. If Y is finite, then G_Y^α is isomorphic to a subalgebra of G_X^α generated by a finite subset of X, which is necessarily free in $\mathbf{V}_\alpha$. If Y is infinite, then every subalgebra of G_Y^α generated by a countable subset of Y is free in $\mathbf{V}_\alpha$; it follows that G_Y^α is free itself.

The characterization of the elements of G_Y^α follows from a similar characterization of the sets of words that are of the form $\mathcal{O}_X(t)$ for a term t. $\square$

4.3. Example. Let $n=2$ and α be the congruence of M generated by the pairs $\langle F_1F_1,F_2F_2\rangle$ and $\langle F_1F_2,F_2F_1\rangle$. Then α is a cancellative and length preserving congruence (we have $e\ \alpha\ f$ if and only if $|e|=|f|$ and the numbers of occurrences of F_1 in e and in f are of the same parity). We have $F_1x+F_1(F_1y+F_2z)=F_1x+F_2F_2y+F_2F_1z\in G_Y^\alpha$, while $F_1x+F_1y\notin G_Y^\alpha$. This shows that $u+e(F_1y_1+\ldots F_ny_n)\in G_Y^\alpha$ does not necessarily imply $u+ex\in G_Y^\alpha$.

If α is a length preserving congruence of M, then it makes sense to define the depth of an element $ey\in H_Y^\alpha$, for any $e\in M$ and $y\in Y$, to be the length of e. For an arbitrary element u of H_Y^α, the minimal depth of u is (defined to be) the minimum of the depths of its summands and the maximal depth of u is the maximum of the depths of its summands. We denote by $\partial(u)$ the maximal and by $\partial'(u)$ the minimal depth of u.

4.4. Lemma. *Let α be a length preserving congruence of M and Y be a nonempty set. Let $m\geq 0$ and $u\in G_Y^\alpha$ be an element of minimal depth $m+1$. If u can be expressed as $u=w+eF_1y_1+\cdots+eF_ny_n$, where e is of length m and $y_i\in Y$, then $w+ey\in G_Y^\alpha$ for any $y\in Y$.*

Proof. Since $u\in G_Y^\alpha$, there exists a linear term t and a homomorphism φ of T into G_Y^α such that φ maps X into Y and $u=\varphi(t)$. There are words $e_1,\ldots,e_n\in\mathcal{O}_X(t)$ with $e_i\ \alpha\ eF_i$ and $y_i=\varphi(t[e_i])$. Put $x_i=t[e_i]$. Every occurrence of a variable in t is of length at least $m+1$. From this it follows that every word of length $m+1$ belongs to $\mathcal{O}(t)$. In particular, $eF_1,\ldots,eF_n$ are elements of $\mathcal{O}(t)$. Denote by t' the (linear) term obtained from t by replacing, for any $i\in\{1,\ldots,n\}$, the subterm

at eF_i with the variable x_i, and the variable x_i with the subterm at eF_i. Using the definition of $\mathbf{E}_\alpha$ it is easy to see that $\langle t, t'\rangle \in \mathbf{E}_\alpha$, so that $\varphi(t') = \varphi(t) = u$. Denote by t'' the term obtained from t' by replacing the subterm $Fx_1 \dots x_n$ at e with a new variable x. Clearly, $w + ey = \psi(t'')$ where ψ is the homomorphism of T into G^α_Y with $\psi(x) = y$ and $\psi(z) = \varphi(z)$ for any $z \in X - \{x\}$. Consequently, $w + ey \in G^\alpha_Y$. $\square$

4.5. Lemma. *Let α be a length preserving congruence of M and Y be a nonempty set. Let $w \in H^\alpha_Y$, $u \in G^\alpha_Y$ and $e \in M$ be such that $w + eu \in G^\alpha_Y$ and $\partial(eu) \leq \partial'(w + eu)$. Then $w + ey \in G^\alpha_Y$ for any $y \in Y$.*

Proof. By induction on the number of summands of u. If $u \in Y$, it is clear. Otherwise, we can write $u = F_1u_1 + \dots + F_nu_n$ where $u_i \in G^\alpha_Y$. Hence $w + eu = w + eF_1u_1 + \dots + eF_nu_n$. Applying the induction assumption n times, we obtain $w + eF_1y_1 + \dots + eF_ny_n \in G^\alpha_Y$ (where $y_i \in Y$). By 4.4, it follows that $w + ey \in G^\alpha_Y$. $\square$

5. Semimodule representations

Let α be a length preserving congruence of M and let $A \in \mathbf{V}_\alpha$ be an algebra without irreducible elements. Put $H = H^\alpha_A$ and $G = G^\alpha_A$ (where A is considered as a set only). Denote by φ the homomorphism of G onto the algebra A extending the identity on A. Let us define a binary relation R on H as follows: $\langle u, v\rangle \in R$ if and only if $u = w + ea$ and $v = w + eF_1a_1 + \dots + eF_na_n$ for some $w \in H$, $e \in M$ and $a = F_A(a_1, \dots, a_n) \in A$. Define a binary relation R' on H by $\langle u, v\rangle \in R'$ if and only if there is a finite sequence $u_1, \dots, u_k$ of elements of H such that $u = u_0$, $v = u_k$ and $\langle u_{i-1}, u_i\rangle \in R \cup R^{-1}$ for all i. Clearly, R' is a congruence of the α-semimodule H; it is the congruence generated by R.

For every $a \in A$ let us fix one n-tuple $\langle q_1(a), \dots, q_n(a)\rangle$ with $a = F_A(q_1(a), \dots, q_n(a))$. For every $a \in A$ and every $e \in M$ define an element $p_e(a)$ of A by induction on the length of e as follows: if $e = \emptyset$, then $p_e(a) = a$; if $e = fF_i$, then $p_e(a) = q_ip_f(a)$. For every $a \in A$ and every nonnegative integer k put

$$C(k, a) = \sum_{e \in L_k} ep_e(a),$$

where L_k denotes the set of the words of length k. For every element $u = e_1a_1 +$

$\cdots + e_k a_k \in H$ and every integer $m \geq \partial(u)$ put

$$D(m,u) = e_1 C(m - |e_1|, a_1) + \cdots + e_k C(m - |e_k|, a_k).$$

5.1. Lemma. *The following are true:*

(1) $C(k,a) \in G$ *and* $\varphi(C(k,a)) = a$ *for any* $a \in A$. *We have* $\partial(C(k,a)) = \partial'(C(k,a)) = k$.

(2) *If* $u \in G$ *and* $m \geq \partial(u)$, *then* $D(m,u) \in G$ *and* $\varphi(D(m,u)) = \varphi(u)$. *We have* $\partial(D(m,u)) = \partial'(D(m,u)) = m$.

(3) *If* $u, v \in H$ *and* $m \geq \partial(u+v)$, *then* $D(m, u+v) = D(m,u) + D(m,v)$.

(4) *If* $u \in H$, $e \in M$ *and* $m \geq \partial(eu)$, *then* $D(m, eu) = eD(m - |e|, u)$.

(5) *Let* $\langle u, v\rangle \in R$. *If* $u \in G$, *then* $v \in G$ *and* $\varphi(u) = \varphi(v)$.

(6) *Let* $\langle u, v\rangle \in R$ *and* m *be an integer such that* $m \geq \partial(u)$ *and* $m \geq \partial(v)$. *If one of the elements* $D(m,u)$ *and* $D(m,v)$ *belongs to* G, *then both belong to* G *and* $\varphi(D(m,u)) = \varphi(D(m,v))$.

(7) *Let* a, b *be two elements of* A *such that* $\langle a, b\rangle \in R'$. *Then* $a = b$.

Proof. The first five assertions are easy to prove. Let us remark, however, that (according to Example 4.3), $\langle u, v\rangle \in R$ and $v \in G$ do not necessarily imply $u \in G$.

Let us prove (6). We have $u = w + ea$ and $v = w + eF_1 a_1 + \cdots + eF_n a_n$ for some $w \in H$, $e \in M$ and $a = F_A(a_1, \ldots, a_n) \in A$. Hence $D(m,u) = D(m,w) + eD(m - |e|, a)$ and $D(m,v) = D(m,w) + eD(m - |e|, F_1 a_1 + \cdots + F_n a_n)$. If either of these two elements belongs to G, then Lemma 4.5 can be applied to show that $D(m,w) + ea \in G$. We have $\langle D(m,w) + ea, D(m,w) + eF_1 a_1 + \cdots + eF_n a_n\rangle \in R$, so that $D(m,w) + eF_1 a_1 + \cdots + eF_n a_n \in G$ and $\varphi(D(m,w) + ea) = \varphi(D(m,w) + eF_1 a_1 + \cdots + eF_n a_n)$ by (5). We have $D(m,u) = D(m, D(m,w) + ea)$ and $D(m,v) = D(m, D(m,w) + eF_1 a_1 + \cdots + eF_n a_n)$, so both these elements belong to G and have the same images under φ according to (2).

In order to prove (7), let $\langle a, b\rangle \in R'$ and $a, b \in A$. There exists a finite sequence $u_0, \ldots, u_k$ of elements of H such that $a = u_0$, $b = u_k$ and $\langle u_{i-1}, u_i\rangle \in R \cup R^{-1}$ for all i. There exists an integer m with $m \geq \partial(u_i)$ for all i. We have $D(m,a) \in G$ and $\varphi(D(m,a)) = a$ by (2). Similarly, $\varphi(D(m,b)) = b$. By (6) we get $\varphi(D(m,u_0)) = \varphi(D(m,u_1)) = \cdots = \varphi(D(m,u_k))$ (and all these elements belong to G). In particular, $a = \varphi(D(m,a)) = \varphi(D(m,b)) = b$. $\square$

5.2. Theorem. *Let α be a length preserving congruence of M. Then for every algebra $A \in \mathbf{V}_\alpha$ without irreducible elements there exists an α-semimodule $S = S(+, 0, h_1, \dots, h_n)$ such that A is a subset of S and $F_A(a_1, \dots, a_n) = h_1 a_1 + \cdots + h_n a_n$ for all $a_1, \dots, a_n \in A$.*

Proof. According to 5.1(7), the mapping $a \mapsto a/R'$ of A into H/R' is injective. It follows from the definition of R' that the mapping is a homomorphism of A onto the subalgebra G/R' of H/R' (with respect to the signature $\{F\}$). So, an isomorphic copy of H/R' serves the purpose. $\square$

5.3. Theorem. *Let α be a length preserving, left cancellative congruence of M satisfying the following condition:*

(∗) *If a word e and an integer $i \in \{1, \dots, n\}$ are such that for any $j \in \{1, \dots, n\}$ there exists a word f_j with $F_i f_j \; \alpha \; eF_j$, then there exists a word g such that $F_i g \; \alpha \; e$.*

Then for every algebra $A \in \mathbf{V}_\alpha$ without irreducible elements there exists an α-semimodule $S = S(+, 0, h_1, \dots, h_n)$ such that $h_1, \dots, h_n$ are injective endomorphisms of $S(+, 0)$, A is a subset of S and $F_A(a_1, \dots, a_n) = h_1 a_1 + \cdots + h_n a_n$ for all $a_1, \dots, a_n \in A$.

Proof. With respect to the proof of Theorem 5.2, it is sufficient to show that $\langle F_i u, F_i v\rangle \in R'$ implies $\langle u, v\rangle \in R'$ for any $i \in \{1, \dots, n\}$.

Let us prove first that if p, q, p' are three elements of H such that $\langle p, q\rangle \in R \cup R^{-1}$ and $p = F_i p'$, then there exists an element q' with $\langle p', q'\rangle \in R \cup R^{-1}$ and $q = F_i q'$. In the case $\langle p, q\rangle \in R$ it is evident, so let $\langle q, p\rangle \in R$. We have $q = w + ea$ and $p = w + eF_1 a_1 + \cdots + eF_n a_n$ for some $w \in H$, $e \in M$ and $a = F_A(a_1, \dots, a_n) \in A$. Since $p = F_i p'$, we have $w = F_i w'$ for some $w' \in H$, $eF_j a_j = F_i f_j a_j$ for some words f_j $(j = 1, \dots, n)$, and $p' = w' + f_1 a_1 + \cdots + f_n a_n$. Hence $eF_j \; \alpha \; F_i f_j$ for all j. By (∗) there exists a word g such that $F_i g \; \alpha \; e$. Since α is left cancellative, $F_i g F_j \; \alpha \; eF_j \; \alpha \; F_i f_j$ implies $gF_j \; \alpha \; f_j$. Put $q' = w' + ga$. Then $\langle q', p'\rangle = \langle w' + ga, w' + gF_1 a_1 + \cdots + gF_n a_n\rangle \in R$ and $F_i q' = F_i w' + F_i ga = w + ea = q$.

If $\langle F_i u, F_i v\rangle \in R'$, then there is a finite sequence $u_0, \dots, u_k$ with $F_i u = u_0$, $F_i v = u_k$ and $\langle u_{j-1}, u_j\rangle \in R \cup R^{-1}$ for all j. According to the previous observation, there are elements $u'_0, \dots, u'_k$ such that $u'_0 = u$, $u_j = F_i u'_j$ for all j and $\langle u'_{j-1}, u'_j\rangle \in$

$R \cup R^{-1}$ for all j. Now $F_i u'_k = F_i v$ implies $u'_k = v$; this follows from the left cancellation property of α. We get $\langle u, v\rangle \in R'$. $\square$

We denote by $\hat{M}$ the free group over $\{F_1, \dots, F_n\}$. The free monoid M is a submonoid of $\hat{M}$. For a congruence α of M, denote by $\hat{\alpha}$ the congruence of $\hat{M}$ generated by α. We say that $\hat{\alpha}$ extends α if $\alpha = \hat{\alpha} \cap (M \times M)$. Clearly, if $\hat{\alpha}$ extends α, then α is a cancellative congruence of M.

By an $\hat{\alpha}$-semimodule we mean a universal algebra of the signature $\{+, 0, F_1, \dots, F_n, F_1^{-1}, \dots, F_n^{-1}\}$, satisfying all the identities for α-semimodules and, moreover,

$$F_i F_i^{-1} x \approx F_i^{-1} F_i x \approx x$$

for $i = 1, \dots, n$. Clearly, the class of $\hat{\alpha}$-semimodules is a variety; it is finitely based whenever α is a finitely generated congruence.

Similarly as in the case of α-semimodules, every $\hat{\alpha}$-semimodule can be considered as an algebra of signature $\{F\}$ with respect to the operation $\langle a_1, \dots, a_n\rangle \mapsto F_1 a_1 + \cdots + F_n a_n$. The algebra again belongs to $\mathbf{V}_\alpha$.

The free $\hat{\alpha}$-semimodule over a nonempty set Y is the set of formal expressions $\sum_{i=1}^r e_i y_i$ where $r \geq 0$, $y_i \in Y$ and $e_i \in \hat{M}$; we have $\sum_{i=1}^r e_i y_i = \sum_{j=1}^s f_j z_j$ if and only if $r = s$ and there is a permutation h of $\{1, \dots, r\}$ such that $y_i = z_{h(i)}$ and $e_i \;\hat{\alpha}\; f_{h(i)}$ for all i. If $\hat{\alpha}$ is an extension of α, then the $\{F\}$-subalgebra generated by Y is isomorphic with G_Y^α and can be identified with G_Y^α.

5.4. Theorem. *Let α be a length preserving congruence of M such that $\hat{\alpha}$ extends α and the following condition is satisfied:*

($\hat{*}$) *If $e \in \hat{M}$ is such that for any $i \in \{1, \dots, n\}$ there exists a word $e_i \in M$ with $\langle eF_i, e_i\rangle \in \hat{\alpha}$, then there exists a word $f \in M$ such that $\langle e, f\rangle \in \hat{\alpha}$.*

Then for every algebra $A \in \mathbf{V}_\alpha$ without irreducible elements there exists an $\hat{\alpha}$-semimodule $S = S(+, 0, h_1, \dots, h_n, h_1^{-1}, \dots, h_n^{-1})$ such that A is a subset of S and $F_A(a_1, \dots, a_n) = h_1 a_1 + \cdots + h_n a_n$ for all $a_1, \dots, a_n \in A$.

Proof. Denote by $\hat{H}$ the free $\hat{\alpha}$-semimodule over the set A, so that H is the subset of $\hat{H}$ consisting of the elements $\sum e_i a_i$ such that for every i there is a word $f_i \in M$ with $\langle e_i, f_i\rangle \in M$. Let us define a binary relation Q on $\hat{H}$ as follows: $\langle u, v\rangle \in Q$ if and only if $u = w + ea$ and $v = w + eF_1 a_1 + \cdots + eF_n a_n$ for some $w \in \hat{H}$,

$e \in \hat{M}$ and $a = F_A(a_1, \dots, a_n) \in A$. Define Q' by $\langle u, v\rangle \in Q'$ if and only if there is a finite sequence $u_1, \dots, u_k$ of elements of $\hat{H}$ such that $u = u_0$, $v = u_k$ and $\langle u_{i-1}, u_i\rangle \in Q \cup Q^{-1}$ for all i. Clearly, Q' is the congruence of $\hat{H}$ generated by R'.

Let $\langle u, v\rangle = \langle w + ea, w + eF_1a_1 + \dots + eF_na_n\rangle \in Q$. We are going to prove that if one of the elements u and v belongs to H, then they both belong to H and $\langle u, v\rangle \in R$. If $u \in H$, then $w \in H$ and $ea = e'a$ for some $e' \in M$, so everything is clear. Let $v \in H$. Then $w \in H$ and for any $i \in \{1, \dots, n\}$ there exists a word $e_i \in M$ with $\langle eF_i, e_i\rangle \in \hat{\alpha}$. By $(\hat{*})$ we get $ea = fa$ for some $f \in M$. Consequently, $u = w + ea \in H$.

It follows that if $\langle u, v\rangle \in Q'$ and at least one of the elements u and v belongs to H, then they both belong to H and $\langle u, v\rangle \in R'$. In particular, if $a, b \in A$ and $\langle a, b\rangle \in H'$, then $\langle a, b\rangle \in R'$ and $a = b$ by 5.1(7). This means that the mapping $a \mapsto a/Q'$ of A into $\hat{H}/Q'$ is injective and the proof can be finished in the same way as the proof of Theorem 5.2. □

For the purpose of applications, we also need to extend (slightly) the results on semimodule representations for algebras containing a zero element. An element o of an algebra A is said to be a zero element if $F_A(a_1, \dots, a_n) = o$ whenever $a_i = o$ for at least one $i \in \{1, \dots, n\}$.

5.5. Theorem. *Let E be a linear equational theory having a base B such that every equation from B is (e, f)-separating for some e, f and the congruence $\alpha = \mathbf{C}_E$ satisfies conditions (1), (2) and (3) of Theorem 3.4. Then for every model A of E without irreducible elements there exists an α-semimodule $S(+, 0, h_1, \dots, h_n)$ such that A is a subset of S, $F_A(a_1, \dots, a_n) = h_1a_1 + \dots + h_na_n$ for all $a_1, \dots, a_n \in A$, and the following are true:*

(1) *if the algebra A contains a zero element o, then $u + o = o$ and $h_1(o) = \dots = h_n(o) = o$ for all $u \in S$;*

(2) *if $\hat{\alpha}$ extends α and $(\hat{*})$ is satisfied, then $h_1, \dots, h_n$ are automorphisms of $S(+)$.*

Proof. We only need to consider the case when A contains a zero element o. For every element $a \in A$ we have fixed one n-tuple $\langle q_1(a), \dots, q_n(a)\rangle$ with $a = F_A(q_1(a), \dots, q_n(a))$; now we should require that $q_1(o) = \dots = q_n(o) = o$. Then $p_e(o) = o$ for all $e \in M$.

Denote by I the set of all elements $u = \sum e_i a_i \in H$ such that $a_i = o$ for at least one i. Clearly, I is an ideal of $H(+)$. Define a binary relation R'_o on H as follows: $\langle u, v\rangle \in R'_o$ if and only if either $\langle u, v\rangle \in R'$ or there are elements $u', v' \in I$ with $\langle u, u'\rangle \in R'$ and $\langle v, v'\rangle \in R'$. Clearly, R' is a congruence of the α-semimodule H. It is easy to see that if $u \in I \cap G$, then $\varphi(D(m, u)) = o$ for all $m \geq \partial(u)$. Using this observation together with 5.1(6), one can prove that if $a \in A - \{o\}$ and $\langle a, u\rangle \in R'$, then $u \notin I$. Consequently, if a, b are two elements of A such that $\langle a, b\rangle \in R'_o$, then $a = b$. So, an isomorphic copy of H/R'_o is a desired α-semimodule.

If $\hat{\alpha}$ extends α and $(\hat{*})$ is satisfied, the $\hat{\alpha}$-semimodule can be similarly constructed as an isomorphic copy of $\hat{H}/Q'_o$, where Q'_o is the congruence defined by $\langle u, v\rangle \in Q'_o$ if and only if either $\langle u, v\rangle \in Q'$ or $\langle u, u'\rangle, \langle v, v'\rangle \in Q'$ for some u', v' belonging to the ideal of the elements of $\hat{H}$ containing o. □

6. Paramedial groupoids

In this section let $n = 2$. Let us denote by V the variety of paramedial groupoids and by E their equational theory. Put $\alpha = \mathbf{C}_E$, so that α is the congruence of the free monoid M generated by $\langle F_1F_1, F_2F_2\rangle$, and $\hat{\alpha}$ is the congruence of the free group $\hat{M}$ generated by $\langle F_1F_1, F_2F_2\rangle$. It is easy to see that α is a length preserving congruence of M and $\hat{\alpha}$ extends α.

For $e = F_{i_1}^{\varepsilon_1} \dots F_{i_k}^{\varepsilon_k} \in \hat{M}$ put $|e| = \varepsilon_1 + \dots + \varepsilon_k$. It is not difficult to see that $\langle e, f\rangle \in \hat{\alpha}$ if and only if $|e| = |f|$ and both e and f can be reduced, by deleting all occurrences of $F_i^{\varepsilon_1}F_i^{\varepsilon_2}$ for any $i \in \{1, 2\}$ and $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$ (in any order), to two words of the form $F_{i_1}^{\varepsilon_1} \dots F_{i_k}^{\varepsilon_k}$ that can differ in the ε's only. Based on this characterization of $\hat{\alpha}$, one can prove easily that all the conditions of Theorem 5.5 are satisfied. We obtain

6.1. Theorem. *Every paramedial groupoid without irreducible elements belongs to the essential core of the variety of paramedial groupoids. For a paramedial groupoid A without irreducible elements there exist a commutative semigroup $S(+)$ and two automorphisms f, g of $S(+)$ such that $ff = gg$, $A \subseteq S$, $ab = f(a) + g(b)$ for all $a, b \in A$, and $u + o = u$ for all $u \in S$ if o is a zero element of A.* □

A groupoid A is called zeropotent if it contains a zero element o and $aa = o$ for all $a \in A$.

6.2. Corollary. *For every zeropotent paramedial groupoid A without irreducible elements, with zero element o, there exist a commutative semigroup $S(+)$ and two automorphisms f, g of $S(+)$ such that $ff = gg$, $A \subseteq S$, $ab = f(a) + g(b)$ for all $a, b \in A$, and $u + o = o = f(u) + g(u)$ for all $u \in S$.*

Proof. Let S, f, g be as in 6.1. Denote by S' the set of the elements $u \in S$ such that $f(u) + g(u) = o$. We have $A \subseteq S'$, since A is zeropotent. The subset S' is a subsemigroup of $S(+)$, since if u and v are two elements of S', then $f(u + v) + g(u+v) = f(u)+f(v)+g(u)+g(v) = o+o = o$. Also, the subset is closed under f: if $u \in S'$, then $ff(u) + gf(u) = ggu + gf(u) = g(gu + fu) = g(o) = o$. Similarly, S' is closed under g. $\square$

References

1. R.El Bashir, J. Ježek and T. Kepka, *Simple zeropotent paramedial groupoids are balanced* (to appear).
2. J.R. Cho, J. Ježek and T. Kepka, *Simple paramedial groupoids* (to appear).
3. J.R. Cho and T. Kepka, *Finite simple zeropotent paramedial groupoids.*
4. J. Ježek and T. Kepka, *Medial groupoids*, Rozpravy ČSAV, Řada mat. a přír. věd **93/2** (1983), 93pp.
5. J. Ježek and T. Kepka, *Equational theories of medial groupoids*, Algebra Universalis **17** (1983), 174–190.
6. J. Ježek and T. Kepka, *The equational theory of paramedial cancellation groupoids*, to appear.
7. R. McKenzie, G. McNulty and W. Taylor, *Algebras, Lattices, Varieties, Volume I*, Wadsworth & Brooks/Cole, Monterey, CA, 1987.
8. G. Pollák and Á. Szendrei, *Independent basis for the identities of entropic groupoids*, Commentationes Math. Univ. Carolinae **22** (1981), 71–85.

Charles University, Sokolovská 83, 186 00 Praha 8, Czech Republic