Commentationes Mathematicae Universitatis Carolinae

György Pollák; Ágnes Szendrei

Independent basis for the identities of entropic groupoids

Commentationes Mathematicae Universitatis Carolinae, Vol. 22 (1981), No. 1, 71--85

Persistent URL: http://dml.cz/dmlcz/106054

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE

22,1 (1981)

INDEPENDENT BASIS FOR THE IDENTITIES OF ENTROPIC GROUPOIDS

G. POLLÁK, Á. SZENDREI

Abstract: The variety E of entropic groupoids, which is generated by any of the algebras $\mathcal{G}_{r,s} = \langle \mathbb{R}; \circ \rangle$ where $\mathbb{R}$ is the set of real numbers, $r,s \in \mathbb{R}$ are algebraically independent and $x \circ y = rx+sy$, is known to be not finitely based [1]. Here we give an independent basis for the identities of E .

Key words and phrases: variety, identity, equational theory, basis (of identities), independent basis, entropic groupoid.

Classification: Primary 08B05
Secondary 20L05

In [1] Ježek and Kepka describe the equational theory of entropic groupoids. In particular it follows that the algebra $\mathcal{O}\!\mathcal{l} = \langle A; \circ \rangle$ defined on the free commutative ring A with free generators a_0, a_1 by $x \circ y = a_0x + a_1y$, generates the variety E of entropic groupoids. They also show that the equational theory of E (and hence of $\mathcal{O}\!\mathcal{l}$) is not finitely based. Here we construct an independent basis for the equational theory of E . These investigations concern also a question of Fajtlowicz and Mycielski[2] asking whether the groupoids $\mathcal{G}_{r,s} = \langle \mathbb{R};\circ\rangle$ defined on the set $\mathbb{R}$ of real numbers by $x\circ y = rx+sy$ have finite bases for their identities. Clearly, if r and s are algebraically independent then $\mathcal{G}_{r,s}$ generates the variety E, hence its equational theory is not finitely based.

We use the terminology and notations of [3]. Since all algebras occurring are groupoids, we omit all references to the type. In particular, for any cardinal β, $P^{(\beta)}$ stands for the set of polynomial symbols of type $\langle 2\rangle$ with variables $\{x_\gamma\colon \gamma<\beta\}$. Clearly, $\mathcal{P}^{(\beta)} = \langle P^{(\beta)};\circ\rangle$ is the free groupoid on β generators. For $p,p'\in P^{(\beta)}$, $p \equiv p'$ means that p and p' coincide.

Let R, A and M denote the free unitary ring, free unitary commutative ring and free monoid with free generators a_0,a_1, respectively. (We consider M to be a subset of R.) The length of a word $w\in M$ is denoted by $|w|$. Define the entropic groupoids $\mathcal{R} = \langle R;\circ\rangle$ and $\mathcal{A} = \langle A;\circ\rangle$ by $x\circ y = a_0x+a_1y$. Let $\alpha\colon R\to A$ be the natural ring homomorphism with $a_i\alpha = a_i$ $(i<2)$. Clearly, α is also a groupoid homomorphism $\mathcal{R}\to\mathcal{A}$. For any $i<\omega$ let $\varphi_i\colon \mathcal{P}^{(\omega)}\to\mathcal{R}$ be the natural homomorphism with $x_i\varphi_i = 1$ and $x_j\varphi_i = 0$ if $j\neq i$. Further, set $\varphi = \sum_{i<\omega}\varphi_i$. It is not hard to show that for any $p,q\in P^{(\omega)}$,

(*) $p\equiv q$ iff for every $i<\omega$, $p\varphi_i = q\varphi_i$;

(**) p and q have the same parenthesis structure, i.e. $p(x_0,\dots,x_0)\equiv q(x_0,\dots,x_0)$, iff $p\varphi = q\varphi$.

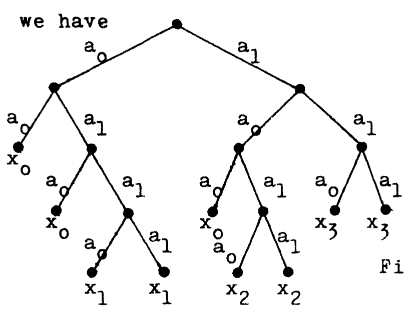
To see this, and also to make it easier to follow the rest of the paper, it is worth noting what the homomorphisms

φ_i mean pictorially. There is a natural way to represent a polynomial symbol in $P^{(\omega)}$ by a binary tree as follows: to x_i $(i<\omega)$ we assign the one-point tree

$$\overset{\bullet}{x_i}$$

and to any polynomial symbol $p\circ q$ we assign the tree arising from $\overset{\bullet}{\bigwedge}$ by attaching to its left and right branches the trees corresponding to p and q, respectively. Now, consider the tree of a polynomial symbol $p\in P^{(\omega)}$, and label all branches going to the left by a_o and all branches going to the right by a_1. In this manner, the paths of the tree of p can be labelled by words from M and every vertex is uniquely characterized by the word corresponding to the path going downwards to it. This word will be called the <u>weight</u> of the vertex. Since the subterms of p are in a natural one-to-one correspondence with the vertices of the tree of p, we can also speak about the weight of a subterm of p. In particular, the variables are also subterms of p. Now it is easy to see that for any $i<\omega$, $p\varphi_i$ is nothing else than the sum of the weights of all occurrences of the variable x_i.

<u>Example</u>. For $p\equiv(x_o\circ(x_o\circ(x_1\circ x_1)))\circ((x_o\circ(x_2\circ x_2))\circ(x_3\circ x_3))$ we have



$$p\varphi_o = a_o^2 + a_oa_1a_o + a_1a_o^2\ ,$$
$$p\varphi_1 = a_oa_1^2a_o + a_oa_1^3\ ,$$
$$p\varphi_2 = a_1a_oa_1a_o + a_1a_oa_1^2\ ,$$
$$p\varphi_3 = a_1^2a_o + a_1^3\ ,$$
$$p\varphi_n = 0 \qquad (n \geq 4)$$

Figure 1

Clearly, for any $p \in P^{(\omega)}$ a variable x_i occurs in p iff $p\varphi_i \neq 0$. Put $\nu(p) = \{i<\omega: p\varphi_i \neq 0\}$. For any mapping $\psi: \nu(p) \to \{i: i<\omega\}$ we denote by p^{ψ} the polynomial symbol arising from p by substituting $x_{i\psi}$ for x_i for all $i \in \nu(p)$.

Proposition 1. For any $p,q \in P^{(\omega)}$, the identity $p=q$ is in $\mathrm{Id}(E)$ if and only if $p\varphi_i\alpha = q\varphi_i\alpha$ holds for all $i<\omega$.

Proof: The statement follows from the fact that for any $p \in P^{(\omega)}$, $p_{\alpha} = \sum_{i<\omega}(p\varphi_i\alpha)x_i$. The proof is straightforward by induction.

Example. Figure 2 shows the tree of a polynomial symbol q for which $p=q$ belongs to $\mathrm{Id}(E)$ (p is the polynomial symbol in Figure 1).

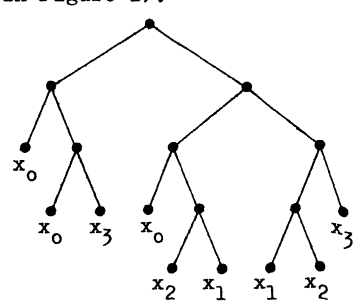


Figure 2

Let $\bar{P}$ denote the set of all $p \in P^{(\omega)}$ in which every x_i $(i<\omega)$ occurs at most once; i.e. $p \in \bar{P}$ iff $p \in P^{(\omega)}$ and $p\varphi_i \in M$ for every $i \in \nu(p)$. Denote by $\tilde{P}$ the subset of $\bar{P}$ consisting of all $p \in \bar{P}$ such that $\nu(p) = \{i: i<n\}$ for some $n<\omega$, and for every $i,j \in \nu(p)$, $i>j$ iff either

$|p\varphi_i| < |p\varphi_j|$ or $|p\varphi_i| = |p\varphi_j|$ and $p\varphi_j$ precedes $p\varphi_i$ in the lexicographic order. Pictorially, this means that a polynomial symbol belongs to $\tilde{P}$ iff in its tree the variables $x_0, x_1, x_2, \ldots$ are attached to the branches sequentially by levels, starting from the bottom, and within one level from the left to the right (see Figure 3).

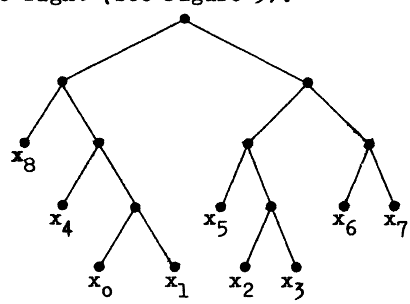


Figure 3

Obviously, for every $p \in \bar{P}$ there is a (unique) one-to-one mapping $\pi: \nu(p) \to \{i: i < \omega\}$ such that $p^{\pi} \in \tilde{P}$. Making use of (*) and (**) it is not hard to see that every polynomial symbol $p \in \tilde{P}$ is uniquely determined by $p\varphi$.

<u>Proposition 2</u>. If $p=q$ $(p,q \in P^{(\omega)})$ is in Id(E) then there exist $p' \in \tilde{P}$ and $q' \in \bar{P}$ such that $p' = q'$ is also in Id(E) and $p' = q' \vdash p=q$.

<u>Example</u>. Let p and q be the polynomial symbols in Figures 1 and 2, respectively. Then $p=q$ is in Id(E) and the polynomial symbol p' in Figure 3 is the unique one in $\tilde{P}$ such that $p'\varphi = p\varphi$. Figure 4 shows two possible choices for q' satisfying the requirements of Proposition 2.

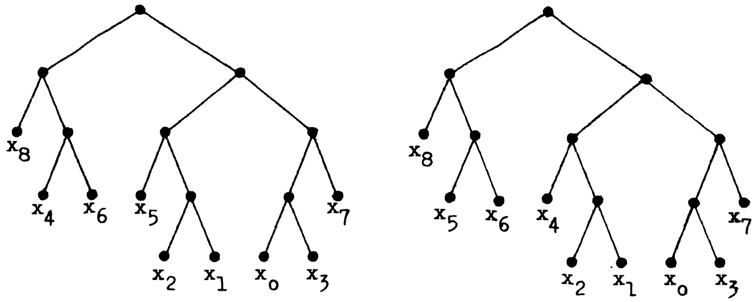


Figure 4

<u>Proof</u>: Let $p' \in \tilde{P}$ be the unique polynomial symbol such that $p'\varphi = p\varphi$ and choose $q' \in \tilde{P}$ so that for any $i < \nu(p')$, if $p'\varphi_i$ is an addend in $p\varphi_j$ then $q'\varphi_i$ be an addend in $q\varphi_j$ such that $q'\varphi_i\alpha = p'\varphi_i\alpha$ (Proposition 1 ensures the existence of such a q'). Then, clearly, $p' = q'$ is in $\mathrm{Id}(E)$ and $p=q$ arises from $p'=q'$ by substituting new (not necessarily distinct) variables.

Let us introduce the following notations: if $w \in M$, say $w = a_{i_0} \dots a_{i_{n-1}}$, and $k \leq n$, put

$$w_k = a_{i_k}, \quad (w)_k = a_{i_0} \dots a_{i_{k-1}}, \quad {}_k(w) = a_{i_k} \dots a_{i_{n-1}},$$

$$\overline{(w)_k} = (w)_{k-1} a_{1-i_{k-1}} \quad \text{and} \quad w^* = w + \sum_{k=1}^{n} \overline{(w)_k} .$$

It is easy to see that for the polynomial symbols $s[w] \in P^{(1)}$ $(w \in M)$ defined by $s[1] \equiv x_0$ and for $n \geq 1$ by $s[w] \equiv$ $\equiv s[{}_1(w)] \circ x_0$ or $x_0 \circ s[{}_1(w)]$ according to whether $i_0 = 0$ or 1, we have $s[w]\varphi = w^*$.

Let $u, v \in M$, $|u| = n$, $|v| = m$. Clearly, there exists a polynomial symbol q such that $q\varphi = a_0 u^* + a_1 v^*$ (e.g.,

$s[u]\circ s[v]$ is one). Denote by $t[a_o u, a_1 v]$ the unique $p\in\tilde{P}$ with $p\varphi = a_o u^* + a_1 v^*$. Observe that these polynomial symbols have exactly 2 subterms of the form $x_i\circ x_j$ $(i,j<\omega)$.

Example. Figure 5 shows the tree of $t[a_o a_1 a_o a_1, a_1^2 a_o^2]$.

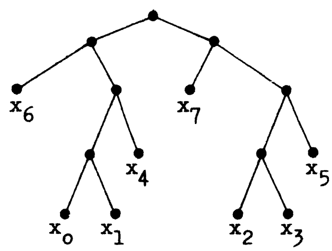


Figure 5

Clearly, if $u_{n-1} = a_i$ and $v_{m-1} = a_j$ then

$$t[a_o u, a_1 v]\varphi_i = a_o u \quad\text{and}\quad t[a_o u, a_1 v]\varphi_{j+2} = a_1 v.$$

Denote by $\sigma(a_o u, a_1 v)$ the identity $t[a_o u, a_1 v] = t^{(i,j+2)}[a_o u, a_1 v]$ where $(i,j+2)$ is a transposition. Put

$$\Sigma_o = \{\sigma(u,v)\colon u,v\in M,\ u_o = a_o,\ v_o = a_1,\ u\alpha = v\alpha\}.$$

Obviously, for $\sigma(u,v)\in\Sigma_o$ we have $|u| = |v|$. This number will be called the depth of $\sigma(u,v)$.

Lemma 1. If $p\in\bar{P}$ and $k,\ell\in\nu(p)$ such that $p\varphi_k\alpha = p\varphi_\ell\alpha$ then we have $\sigma(u,v)\vdash p = p^{(k,\ell)}$ for some $\sigma(u,v)\in\Sigma_o$ of depth $\leqq |p\varphi_k|$.

Proof: Let $|p\varphi_k| = |p\varphi_\ell| = n$, ${}_{n-1}(p\varphi_k) = a_i$ and ${}_{n-1}(p\varphi_\ell) = a_j$. We proceed by induction on the rank of p. Our claim being trivial if p is a variable, we can suppose that it holds for all polynomial symbols of rank smaller than that of p. We can also assume that $k \neq \ell$, whence $p\varphi_k \neq p\varphi_\ell$. If $(p\varphi_k)_o = (p\varphi_\ell)_o$ then x_k and x_ℓ occur in the same subterm of p, so the lemma follows from the induction hypothesis. Suppose now that they occur in different subterms, say $(p\varphi_k)_o = a_o$ and $(p\varphi_\ell)_o = a_1$. Then it is not hard to show that

$$p \equiv t[p\varphi_k, p\varphi_\ell](p_o, p_1, \ldots) \quad \text{with} \quad p_i \equiv x_k \quad \text{and} \quad p_{j+2} \equiv x \;,$$

whence the lemma follows.

<u>Proposition 3</u>. Σ_o is a basis of $Id(E)$.

<u>Proof</u>: By Proposition 2 it suffices to show that for any identity $p=q$ in $Id(E)$ with $p \in \tilde{P}$, $q \in \bar{P}$, we have $\Sigma_o \vdash p=q$. We proceed by induction. In view of $(*)$ we shall be done if we prove the following statement: if $p\varphi_k \neq q\varphi_k$ and for all $j > k$ we have $p\varphi_j = q\varphi_j$ then there exists a $q' \in \bar{P}$ such that $\Sigma_o \vdash q=q'$ and $p\varphi_i = q'\varphi_i$ for all $i \geq k$.

Let $d = |p\varphi_k|$. Since $p \in \tilde{P}$, by assumption we have $p\varphi_j = q\varphi_j$ whenever $|p\varphi_j| < d$. Therefore there exists a polynomial symbol $r \in P^{(\omega)}$ such that

$$p \equiv r(p_o, p_1, \ldots, p_m, x_{k+1}, \ldots),$$
$$q \equiv r(q_o, q_1, \ldots, q_m, x_{k+1}, \ldots)$$

and $|r\varphi_o| = \ldots = |r\varphi_m| = d$. Since $p\varphi_k \neq q\varphi_k$, we may suppose without loss of generality that $p_o \equiv x_k$ and $q_1 \equiv x_k$. On the other hand, $p=q$ belongs to $Id(E)$, so that by Proposition 1 we have $p\varphi_k\alpha = q\varphi_k\alpha$, i.e. $r\varphi_o\alpha = r\varphi_1\alpha$. Then, by Lemma 1,

$\Sigma_o \vdash r = r^{(0,1)}$, whence for

$$q' \equiv r(q_1, q_o, q_2, \ldots, q_m, x_{k+1}, \ldots)$$

we have $\Sigma_o \vdash q = q'$. Clearly, q' also satisfies the other requirement.

Lemma 2. Let $u \in M$, $|u| = n$, and let $\sigma(u,v) \in \Sigma_o$ be such that for some $0 < k < n$ we have $\overline{(u)_{k+1}} = (v)_{k+1}$. Then $\sigma(u,v)$ can be derived from identities of depths $< n$ in Σ_o.

Proof: Let $u = a_{i_o} \ldots a_{i_{n-1}}$, $v = a_{j_o} \ldots a_{j_{n-1}}$ and put $i = i_{n-1}$, $j = j_{n-1}$. Since $u\alpha = v\alpha$, necessarily $k < n-1$. It is not hard to check that

$$\begin{aligned} t[u,v] &\equiv t[(u)_{k+1},(v)_{k+1}](p_o,\ldots,p_3,x_{2n-2k+2},\ldots,x_{2n-1}) \equiv \\ &\equiv t[\overline{(u)_{k+1}},(v)_{k+1}](p_o,\ldots,p_3,x_{2n-2k+2},\ldots,x_{2n-1}) \end{aligned}$$

and the variables x_i, x_{j+2} occur in p_{i_k}, p_{j_k+2}, respectively. Let q be the polynomial symbol arising from $t[u,v]$ by interchanging p_{1-i_k} and p_{j_k+2}. Clearly,

$$\sigma(\overline{(u)_{k+1}},(v)_{k+1}) \vdash t[u,v] = q, \quad t^{(i,j+2)}[u,v] = q^{(i,j+2)} .$$

Therefore it remains to show that the identity $q = q^{(i,j+2)}$ can be derived from an identity of depth $< n$ in Σ_o. However, this follows from Lemma 1 since by construction

$$q\varphi_i = t[u,v]\varphi_i \quad \text{and} \quad q\varphi_{j+2} = \overline{(u)_{k+1}}(p_{j_k+2}\varphi_{j+2}),$$

implying by $k > 0$ that $(q\varphi_i)_1 = (q\varphi_{j+2})_1$. The proof is complete.

Let

$$\Sigma_1 = \{\sigma(u,v) \in \Sigma_0 \colon u = u'w,\ v = v'w,\ (u)_k\alpha \neq (v)_k\alpha \text{ for } 0<k<|u'|, \text{ and if } (a_i(u)_k)\alpha = (a_{1-i}(v)_k)\alpha \text{ for some } i<2,\ k<|u'| \text{ then } u_k \neq v_k\}\ .$$

Proposition 4. Σ_1 is a basis of $Id(E)$.

Proof: In virtue of Proposition 3 it suffices to prove that $\Sigma_1 \vdash \Sigma_0$. Provisionally, denote by Ψ the set of all identities in Σ_0 that can be derived from Σ_1. Obviously, $\Sigma_1 \subseteq \Psi \subseteq \Sigma_0$. Suppose that, contrary to our claim, $\Psi \neq \Sigma_0$ and choose a $\sigma(u,v) \in \Sigma_0 - \Psi$ of minimum depth. Let m be the smallest positive integer such that $(u)_m\alpha = (v)_m\alpha$, and put $(u)_m = u'$, $(v)_m = v'$. Further, let $u = u'u''$, $v = v'v''$. Since $\sigma(u,v) \notin \Sigma_1$, either $u'' \neq v''$ or there exist k and i $(k<m,\ i<2)$ such that $(a_i(u)_k)\alpha = (a_{1-i}(v)_k)\alpha$ and $u_k = v_k$. We show that in both cases $\sigma(u,v)$ satisfies the hypotheses of Lemma 2, so that it can be derived from identities of depths $<|u|$ in Σ_0, which by the minimum property of $\sigma(u,v)$ implies that $\Sigma_1 \vdash \sigma(u,v)$, contradicting our choice.

Indeed, if $u'' \neq v''$, say $u''_\ell \neq v''_\ell$ $(\ell < |u''|)$ and ℓ is minimal with respect to this property then

$$\overline{(u)_{n+\ell+1}}\alpha = ((u)_{n+\ell}v'')\alpha = (v)_{n+\ell+1}\alpha\ .$$

If, in turn, $(a_i(u)_k)\alpha = (a_{1-i}(v)_k)\alpha$ and $u_k = v_k$ for some $k<m$, $i<2$ then by symmetry we can assume $u_k = v_k = a_i$; so

$$(u)_{k+1}\alpha = ((v)_k a_{1-i})\alpha = \overline{(v)_{k+1}}\alpha\ ,$$

concluding the proof.

Let

$$\Sigma = \{\sigma(u,v) \in \Sigma_1 : \text{ at least one of } u,v \text{ ends with } a_0\}.$$

Now we are ready to state our main theorem.

<u>Theorem</u>. Σ is an independent basis of $\mathrm{Id}(E)$.

<u>Corollary</u>. E has no finite basis for its identities.

The crucial part of the proof of the Theorem will be formulated in a separate lemma below. Denote by X the set of all pairs (u,v) such that $\sigma(u,v) \in \Sigma$. Let $(u,v) \in X$ and $u = a_{i_0} \dots a_{i_{n-1}}$, $v = a_{j_0} \dots a_{j_{n-1}}$. Clearly, by the definition of Σ we have

(i) $u\alpha = v\alpha$;

(ii) $i_0 = 0$, $j_0 = 1$;

(iii) for all $0<k<n$, if $(u)_k\alpha = (v)_k\alpha$ then $i_k = j_k$;

(iv) if there exist $i<2$, $0<k<n$ such that $((u)_k a_i)\alpha = ((v)_k a_{1-i})\alpha$ then $i_k \neq j_k$.

<u>Lemma 3</u>. Let $(u,v) \in X$ and $p \in P^{(\omega)}$ such that $p\varphi\alpha = t[u,v]\varphi\alpha$. Then $p\varphi = t[u,v]\varphi$.

<u>Proof</u>: From the definition of $t[u,v]$ it follows immediately that

$$T = t[u,v]\varphi = u + \sum_{j=2}^{n} \overline{(u)}_j + v + \sum_{j=2}^{n} \overline{(v)}_j .$$

Thus, for $2 \leqq j < n$, the only words of lengths j entering the sum are $\overline{(u)}_j$ and $\overline{(v)}_j$. Now let $p\varphi\alpha = T\alpha$. We have to show that every addend of T occurs in $p\varphi$, too. We proceed by induction on the lengths of the words. From (ii) and

(iv) it follows that either $\overline{(u)}_2 = a_o a_1$, $\overline{(v)}_2 = a_1 a_o$ or $\overline{(u)}_2 = a_o^2$, $\overline{(v)}_2 = a_1^2$. Since $p\varphi\alpha = T\alpha$ and the addends of $p\varphi$ are distinct, in both cases $\overline{(u)}_2$ and $\overline{(v)}_2$ must occur in $p\varphi$.

Suppose now that $\overline{(u)}_j$ and $\overline{(v)}_j$ enter $p\varphi$ for some $2 \leq j < n$. First we show that any addend w of length $j+1$ in $p\varphi$ is of the form $(u)_j a_i$ or $(v)_j a_i$ for some $i < 2$. Indeed, as $\overline{(u)}_j$ and $\overline{(v)}_j$ occur in $p\varphi$, p must have two subterms with weights $(u)_j$ and $(v)_j$, respectively. If either one of these subterms were the product of two terms of lengths ≥ 2, then p would have more than two subterms of lengths 2. However, if $x_k \circ x_\ell$ is a subterm of p then $p\varphi_k\alpha = a_o^{r+1} a_1^s$, $p\varphi_\ell\alpha = a_o^r a_1^{s+1}$, but $p\varphi\alpha$ contains only two pairs of members of this kind, namely u, $\overline{(u)}_n$ and v, $\overline{(v)}_n$. Thus $p\varphi$ must contain two words of the form $(u)_j a_{i'}$ and $(v)_j a_{i''}$, respectively, if $j < n-1$ and the four words u, $\overline{(u)}_n$, v, $\overline{(v)}_n$ if $j=n-1$. Since $p\varphi\alpha = T\alpha$, $p\varphi$ has no other addend of length $j+1$.

Now we are ready to complete the induction step. If $j = n-1$ then, as we proved in the previous paragraph, every addend of length $j+1=n$ of T must occur in $p\varphi$. Suppose now that $j < n-1$ and $\overline{(u)}_{j+1}$ doesn't enter $p\varphi$. Since $p\varphi\alpha = T\alpha$, $p\varphi$ has an addend w such that $w\alpha = \overline{(u)}_{j+1}\alpha$. By the above statement w equals $(u)_j a_i$ or $(v)_j a_i$ for some $i < 2$. Assume the first. Then, obviously, $u_j \neq a_i$ because else we would have $\overline{(u)}_{j+1} = (u)_j a_i = w$, contrary to the assumption. Hence $\overline{(u)}_{j+1}\alpha = ((u)_j a_{1-i})\alpha \neq w\alpha$, which is not the case. Thus $w = (v)_j a_i$. We can assume that $w \neq \overline{(v)}_{j+1}$ whence $(v)_j a_i = (v)_{j+1}$, $v_j = a_i$. However, then

$\overline{(u)_{j+1}}\alpha = (v)_{j+1}\alpha$, which contradicts (iii) or (iv) depending on whether u_j and v_j (i.e., the last letters of $(u)_{j+1}$ and $(v)_{j+1}$) are distinct or not. This completes the proof of the lemma.

Let $p \in \bar{P}$, $i,j \in \nu(p)$. We shall say that the variables x_i and x_j are <u>linked</u> in p if $x_i \circ x_j$ or $x_j \circ x_i$ is a subterm of p. Equivalently, x_i and x_j are linked iff $p\varphi_i$ and $p\varphi_j$ are of the same length and differ in their last letters only. For example, in the polynomial symbol $t[u,v]$ $(u,v \in M,\ |u| = |v|)$, x_0, x_1 and x_2, x_3 are linked with each other, and they are the only variables which are linked with another one.

<u>Proof of the Theorem</u>: To show that Σ is a basis of $\mathrm{Id}(E)$, by Proposition 4 it suffices to note that if $|u| = |v| = n$ and $u_{n-1} = v_{n-1} = a_1$ then $\sigma(u,v)$ can be derived from Σ as follows:

$$\sigma((u)_{n-1}a_0, (v)_{n-1}a_0) \vdash t[u,v] = t^{(0,2)}[u,v]$$

and

$$\sigma((u)_{n-1}, (v)_{n-1}) \vdash t^{(0,2)}[u,v] = t^{(1,3)}[u,v].$$

Next we prove that Σ is independent. By way of contradiction suppose that for $\sigma(u,v) \in \Sigma$, $\Sigma' = \Sigma - \{\sigma(u,v)\}$ we have $\Sigma' \vdash \sigma(u,v)$. Choose the permutations π, ρ on $\{i : i < 2n\}$ so that the shortest derivation of the identity

$$(***) \qquad t^{\pi}[u,v] = t^{\rho}[u,v]$$

from Σ' be of minimum length among all those of form (***)

for which there exists a variable which is linked with different variables on the two sides. Clearly, such an identity is not contained in Σ'. (Observe that when we replaced Σ_1 by Σ, we omitted exactly those identities from Σ_1 which would have violated this.)

We will arrive at a contradiction by proving that the last step of the shortest derivation of (***) cannot be the application of any one of rules (1)-(5) in [3; p. 381]. This is obvious for (1). By the minimality condition it follows immediately for (2) and (3), too, noticing that if for some $r \in P^{(\omega)}$ we have $\Sigma' \vdash t^{\pi}[u,v]=r$ (and hence $t^{\pi}[u,v]=$ $=r$ belongs to $Id(E)$) then by Lemma 3 and Proposition 1 there exists a permutation τ on $\{i: i<2n\}$ such that $r \equiv t^{\tau}[u,v]$.

If $t^{\pi}[u,v] \equiv p_0 \circ p_1$, $t^{\rho}[u,v] \equiv r_0 \circ r_1$ and $\Sigma' \vdash p_0=r_0$, $p_1=r_1$ then clearly $p_0=r_0$, $p_1=r_1$ belong to $Id(E)$, so by the construction of $t[u,v]$ one easily infers that $p_0 \equiv r_0$ and $p_1 \equiv r_1$. Therefore $\pi=\rho$, contradicting our choice. This settles case (4).

Finally, suppose in the last step of the derivation of (***) rule (5) is applied and, say, the polynomial symbols r_i $(i<m)$ are substituted for the variables x_i $(i<m)$. By the minimality condition at least one of the r_i's is not a variable and hence contains a pair of linked variables, which are linked in $t^{\pi}[u,v]$ and $t^{\rho}[u,v]$, too. On the other hand, from the definition of $t[u,v]$ it follows that $t^{\pi}[u,v]$ and $t^{\rho}[u,v]$ have exactly two linked pairs of variables. Therefore the relation "linkedness" of the vari-

ables in $t^{\pi}[u,v]$ and $t^{\varrho}[u,v]$ coincide, contradicting our assumption. The proof of the Theorem is complete.

Remark. Along the same lines one can easily construct an (infinite) independent basis for the identities of algebras $\langle \mathbb{R};f\rangle$ where f is an n-ary $(n \geq 2)$ operation

$$f(x_0,\dots,x_{n-1}) = \sum_{i<n} r_i x_i$$

whose coefficients r_i $(i<n)$ are algebraically independent.

We are grateful to G. Czédli for his helpful suggestions to make some parts of this paper more readable.

R e f e r e n c e s

[1] J. JEŽEK and T. KEPKA: Medial groupoids, Rozpravy Československe Akad. Věd., Ser. Math. Nat. Sci. (to appear).

[2] S. FAJTLOWICZ and J. MYCIELSKI: On convex linear forms, Algebra Universalis 4(1974), 244-249.

[3] G. GRÄTZER: Universal Algebra, 2nd edition, Springer-Verlag, New York - Heidelberg - Berlin 1979.

Somogyi B. u. 7.
6720 Szeged, Hungary

Bolyai Institute
Aradi vértanuk tere 1.
6720 Szeged, Hungary

(Oblatum 23.7. 1980)