F. BLANCHET-SADRI

On the semidirect product of the pseudovariety of semilattices by a locally finite pseudovariety of groups


<http://www.numdam.org/item?id=ITA_1997__31_3_237_0>
ON THE SEMIDIRECT PRODUCT OF THE
PSEUODOVARIETY OF SEMILATTICES BY A
LOCALLY FINITE PSEUODOVARIETY OF GROUPS (*)

by F. Blanchet-Sadri (1) (2)

Abstract – In this paper, we give a sequence of identities defining the product pseudovariety \( J_1 \ast H \) generated by all semidirect products of the form \( M \ast N \) with \( M \in J_1 \) and \( N \in H \) (here \( J_1 \) is the pseudovariety of semilattice monoids and \( H \) is a locally finite pseudovariety of groups) A sequence of sets of identities ultimately defining \( J_1 \ast G_p \) results (here \( G_p \) is the pseudovariety of \( p \)-groups)

Résumé – Dans cet article, nous donnons une suite d’identités définissant la pseudovariété \( J_1 \ast H \) engendrée par les produits semidirects de la forme \( M \ast N \) où \( M \in J_1 \) et \( N \in H \) (ici \( J_1 \) est la pseudovariété des demi-treillis et \( H \) une pseudovariété de groupes localement finie) Une suite d’ensembles d’identités définissant ultimement \( J_1 \ast G_p \) en résulte (ici \( G_p \) est la pseudovariété des \( p \)-groupes)

1. INTRODUCTION

In this paper, we discuss a technique to produce identities for the semidirect product pseudovariety \( J_1 \ast H \) generated by all semidirect products of the form \( M \ast N \) with \( M \in J_1 \) and \( N \in H \), where \( J_1 \) is the pseudovariety of all semilattice monoids and \( H \) is a locally finite pseudovariety of groups.

The notion of congruence plays a central role in our approach. For any finite alphabet \( A \) denote by \( A^* \) the free monoid generated by \( A \). We say that a monoid \( M \) is \( A \)-generated if there exists a congruence \( \beta \) on \( A^* \) such that \( M \) is isomorphic to \( A^*/\beta \). A pseudovariety of monoids \( \mathbf{V} \) is locally finite if

(*) Received October 1995
(1) Department of Mathematical Sciences, University of North Carolina, Greensboro, NC 27412, USA E-mail blanchet@iris.uncg.edu
(2) This material is based upon work supported by the National Science Foundation under Grant No CCR-9300738 A Research Assignment from the University of North Carolina at Greensboro is gratefully acknowledged I thank Jean-Eric Pin and the referees of preliminary versions of this paper for their very valuable comments and suggestions

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754/97/03/$ 4 00© AFCET-Gauthier-Villars
for any $A$ there are finitely many $A$-generated monoids in $V$. Equivalently, there exists for each $A$ a congruence $\beta_A$ such that an $A$-generated monoid $M$ is in $V$ if and only if $M$ is a morphic image of $A^*/\beta_A$.

Let $H$ be a locally finite pseudovariety of groups. Let $\gamma$ be the congruence generating $H$ for the finite alphabet $A$. The idea is to associate with $J_1 \ast H$ a congruence $\sim_\gamma$ on $A^*$. Section 3 gives a criterion to determine when an identity on $A$ is satisfied in $J_1 \ast H$ with the help of $\sim_\gamma$. This leads to a proof that such $J_1 \ast H$ are locally finite and hence decidable. This criterion follows from Almeida’s semidirect product representation of the free objects in $V \ast W$ in case both $V$ and $W$ have finite free objects [1] (Almeida’s representation is stated in Section 2.1). In Section 5, we give a basis of identities for $J_1 \ast H$ which follows mainly from a result on graphs due to Simon [8] (Simon’s result is stated in Section 4) and the identity criterion of Section 3. In Section 6, we give a sequence of sets of identities ultimately defining the pseudovariety $J_1 \ast G_p$, where $p$ is a prime number and $G_p$ is the pseudovariety of all $p$-groups, that is the pseudovariety of all groups of order $p^k$ for some nonnegative integer $k$.

Related known results include the following. The product $J_1 \ast G$ is generated by the inverse monoids (Margolis and Pin [11]) and is the class of finite monoids in which the idempotents commute (Ash [4]) (here $G$ is the pseudovariety of groups). Blanchet-Sadri and Zhang [6] give identities ultimately defining the pseudovariety $J_1 \ast G_{com}$ where $G_{com}$ denotes the pseudovariety of commutative groups. Irastorza [10] shows that if the pseudovarieties $V$ and $W$ are finitely based, their product may not be.

The techniques in this paper were used in particular by Pin [13] to give a basis of identities for $J_1 \ast J_1$, by Almeida [2] to generalize Pin’s result to iterated semidirect products of finite semilattices, and by Blanchet-Sadri [5] to give a basis of identities for $J_1 \ast J_k$ where $J_k$ denotes the pseudovariety of $\mathcal{J}$-trivial monoids of height $k$.

2. PRELIMINAIRES

We refer the reader to [3, 7, 8, 12] for terms not explicitly defined here.

2.1. Pseudovarieties of monoids

A nonempty class of finite monoids is called a pseudovariety if it is closed under submonoids, morphic images, and finitary direct products. A nonempty
class of monoids is called a variety if it is closed under submonoids, morphic images, and direct products.

As the intersection of a class of pseudovarieties of monoids is again a pseudovariety, and as all finite monoids form a pseudovariety, we can conclude that for every class \( C \) of finite monoids there is a smallest pseudovariety containing \( C \), called the pseudovariety generated by \( C \). Now, if \( C \) is a class of monoids, the smallest variety containing \( C \) is called the variety generated by \( C \).

For a pseudovariety \( V \) and a set \( A \), \( F_{V}(A) \) denotes the free object on \( A \) (or generated by \( A \)) in the variety generated by \( V \). If \( A \) is finite, say \( A = \{a_{1}, \ldots, a_{r}\} \), we often write \( F_{V}(a_{1}, \ldots, a_{r}) \) for \( F_{V}(A) \). In case \( V \) is the pseudovariety of all finite semigroups (respectively all finite monoids), the semigroup (respectively monoid) \( F_{V}(A) \) is usually denoted by \( A^{+} \) (respectively \( A^{*} \)). Elements of \( A^{+} \) are viewed as nonempty words of elements of \( A \), and the multiplication is given by concatenation of words. The monoid \( A^{*} \) includes also the empty word \( 1 \). For a word \( u \in A^{*} \), let \( |u| \) denote the length of \( u \). For words \( u, v, w \in A^{*} \) satisfying \( w = uv \), let \( w \setminus u \) denote the factor \( v \).

2.1.1. Semidirect products of pseudovarieties

Let \( M \) and \( N \) be monoids. It is convenient to write \( M \) additively, without however assuming that \( M \) is commutative. We denote by \( 0 \) (respectively \( 1 \)) the unit element of \( M \) (respectively \( N \)). A left action of \( N \) on \( M \) is a morphism \( \varphi \) from \( N \) into the monoid of monoid endomorphisms of \( M \), where endomorphisms of \( M \) are written on the left.

Given a left action \( \varphi \) of \( N \) on \( M \), we define the semidirect product \( M \rtimes N \) as follows. The elements of \( M \rtimes N \) are pairs \((m, n)\) with \( m \in M \), \( n \in N \). Multiplication is given by the formula

\[
(m, n)(m', n') = (m + nm', nn')
\]

where \( nm' \) represents \( \varphi(n)(m') \). (This is what Eilenberg [8] calls a “unitary” semidirect product.) The multiplication in \( M \rtimes N \) is associative. Thus \( M \rtimes N \) is a monoid with \((0,1)\) as unit element.

We now relate the notion of pseudovariety with that of a semidirect product. Given pseudovarieties of monoids \( V \) and \( W \), we denote by \( V \rtimes W \) the pseudovariety generated by all semidirect products \( M \rtimes N \) with \( M \in V \), \( N \in W \) and with any left action of \( N \) on \( M \). The semidirect product of pseudovarieties of monoids is associative.
PROPOSITION 2.1: (Almeida [1]) Let \( V \) and \( W \) be pseudovarieties of monoids such that \( F_V(A) \) and \( F_W(A) \) are finite for all finite \( A \). Then so is \( V \ast W \). Moreover, for a finite set \( A \), let \( N = F_W(A) \) and \( M = F_V(N \times A) \). Consider the left action of \( N \) on \( M \) defined by \( n(n', a) = (nn', a) \) and the associated semidirect product \( M \ast N \). Then, there is an embedding from \( F_{V \ast W}(A) \) into \( M \ast N \) that maps \( a \) into \(( (1, a), a) \).

2.1.2. Pseudovarieties and sequences of identities

Let \( A \) be a set. A monoid identity on \( A \) is an expression of the form \( u = v \) where \( u, v \in A^* \). A monoid \( M \) satisfies an identity \( u = v \) (or the identity is true in \( M \), or holds in \( M \)), abbreviated by \( M \models u = v \), if for every morphism \( \varphi : A^* \to M \) we have \( \varphi(u) = \varphi(v) \).

A class \( C \) of monoids satisfies \( u = v \), written \( C \models u = v \), if each member of \( C \) satisfies \( u = v \). If \( \Sigma \) is a set of identities, we say \( C \) satisfies \( \Sigma \), written \( C \models \Sigma \), if \( C \models u = v \) for each \( u = v \in \Sigma \). An identity \( u = v \) is deducible from a set of identities \( \Sigma \), abbreviated by \( \Sigma \vdash u = v \), if for every monoid \( M \) we have \( M \models \Sigma \) implies \( M \models u = v \). Here, letters can be erased in monoid identities.

Let \( u_i = v_i, i \geq 1 \) be a sequence of identities. Put \( \Sigma = \{ u_i = v_i \mid i \geq 1 \} \), and define \( V(\Sigma) \) to be the class of finite monoids satisfying \( \Sigma \) or all the identities \( u_i = v_i \). A class \( C \) of finite monoids is said to be defined by \( \Sigma \) (or by the identities \( u_i = v_i, i \geq 1 \)) if \( C = V(\Sigma) \); \( \Sigma \) is said to be a basis for \( C \).

Eilenberg and Schützenberger [9] show that every pseudovariety generated by a single monoid is of the form \( V(\Sigma) \) for some such \( \Sigma \).

2.2. Varieties of sets

Let \( L \) be a subset of \( A^* \). We define a congruence \( \sim_L \) on \( A^* \) as follows: \( u \sim_L v \) holds if \( xuvy \in L \) if and only if \( xvy \in L \) for all \( x, y \in A^* \). The congruence \( \sim_L \) is called the syntactic congruence of \( L \), and the quotient monoid \( A^*/\sim_L \), which we denote by \( M(L) \), is called the syntactic monoid of \( L \). The subset \( L \) of \( A^* \) is saturated for the congruence \( \sim_L \), that is \( u \sim_L v \) and \( u \in L \) imply \( v \in L \). Each pseudovariety of monoids is generated by the syntactic monoids that it contains. The set \( L \) is recognizable if and only if \( M(L) \) is a finite monoid.

Suppose that for each finite alphabet \( A \), a family \( A^*\mathcal{V} \) of recognizable sets of \( A^* \) is given. We then say that \( \mathcal{V} = \{ A^*\mathcal{V} \} \) is a *-variety of sets if it satisfies the following conditions:

- \( A^*\mathcal{V} \) is closed under boolean operations;
If \( L \in A^*V \) and \( a \in A \), then the sets \( a^{-1}L = \{ w \in A^* \mid aw \in L \} \) and \( La^{-1} = \{ w \in A^* \mid wa \in L \} \) are in \( A^*V \);

If \( \varphi : B^* \to A^* \) is a monoid morphism and if \( L \in A^*V \), then \( \varphi^{-1}(L) \in B^*V \).

Pseudovarieties of monoids and *-varieties of sets are in 1–1 correspondence. If \( V \) is a *-variety of sets, then the pseudovariety of monoids generated by \( \{ M(L) \mid L \in A^*V \text{ for some } A \} \) defines the corresponding pseudovariety of monoids \( V \). If \( V \) is a pseudovariety of monoids, then \( A^*V = \{ L \subseteq A^* \mid M(L) \in V \} \) defines the corresponding *-variety of sets \( V \).

3. CONGRUENCES FOR \( J_1 \ast H \)

In this section, we give a criterion to determine when an identity is satisfied in the semidirect product \( J_1 \ast H \) where \( H \) is a locally finite pseudovariety of groups. This criterion is used in Section 5 to obtain a basis of identities for \( J_1 \ast H \).

Let \( A \) be a finite set. For a word \( u \in A^* \), let \( \alpha(u) \) denote the set of elements of \( A \) that occur in \( u \). Then the free object of \( J_1 \) on \( A \) is isomorphic to the quotient \( A^*/\alpha \) where the congruence \( \alpha \) on \( A^* \) is defined by \( u\alpha v \) if and only if \( \alpha(u) = \alpha(v) \). Now, let \( \gamma \) be the congruence of finite index on \( A^* \) such that an \( A \)-generated monoid \( M \) belongs to \( H \) if and only if \( M \) is a morphic image of \( A^*/\gamma \). The free object \( F_H(A) \) is isomorphic to the quotient \( A^*/\gamma \). The pseudovarieties \( J_1 \) and \( H \) have hence finite finitely generated free objects. We denote by \( \pi_\gamma \) the canonical projection from \( A^* \) into \( F_H(A) \) that maps \( a \) onto the generator \( a \) of \( F_H(A) \). If \( u,v \in A^* \), then \( \pi_\gamma(u) = \pi_\gamma(v) \) if and only if \( u\gamma v \).

**Definition 3.1:** Let \( w \in A^* \).

- Let \( \sigma_\gamma : A^* \to (F_H(A) \times A)^* \) be the function defined by
  \[
  \sigma_\gamma(a_1 \ldots a_i) = (1, a_1)(\pi_\gamma(a_1), a_2) \ldots (\pi_\gamma(a_1 \ldots a_{i-1}), a_i)
  \]
  if \( i > 0 \), \( 1 \) otherwise.

- Let \( \sigma_\gamma^w : A^* \to (F_H(A) \times A)^* \) be the function defined by
  \[
  \sigma_\gamma^w(a_1 \ldots a_i) = (\pi_\gamma(w), a_1)(\pi_\gamma(wa_1), a_2) \ldots (\pi_\gamma(wa_1 \ldots a_{i-1}), a_i)
  \]
  if \( i > 0 \), \( 1 \) otherwise.
The sequential function $\sigma_\gamma$ is realized by the transducer whose states are the elements of $F_H(A)$ (1 being the initial state) and whose transitions are given by

$$n \xrightarrow{a/(n,a)} na$$

where $n \in F_H(A)$ and $a \in A$.

We define an equivalence relation on $A^*$ by requesting that

$$u \sim_\gamma v \text{ if and only if } \alpha(\sigma_\gamma(u)) = \alpha(\sigma_\gamma(v)) \text{ and } uv \gamma v.$$  

**Lemma 3.1:** The equivalence relation $\sim_\gamma$ is a congruence of finite index on $A^*$.

**Proof:** Assume $u \sim_\gamma v$ and $u' \sim_\gamma v'$. We have

$$\alpha(\sigma_\gamma(u)) = \alpha(\sigma_\gamma(v)) \text{ and } uv \gamma v$$

and similarly with $u$ and $v$ replaced by $u'$ and $v'$. Since $\gamma$ is a congruence we have $uw' \gamma vv'$. The above and the fact that $\pi_\gamma(u) = \pi_\gamma(v)$ imply that $\alpha(\sigma_\gamma(uw')) = \alpha(\sigma_\gamma(u)\sigma_\gamma(v')) = \alpha(\sigma_\gamma(v)\sigma_\gamma(v')) = \alpha(\sigma_\gamma(vv'))$. Thus $uw' \sim_\gamma vv'$ showing that $\sim_\gamma$ is a congruence. This obviously is a finite congruence since $\alpha$ and $\gamma$ are finite. \hfill \Box

**Lemma 3.2:** If $u = v$ is an identity on $A$, then the following conditions are equivalent:

- $J_1 \star H \models u = v$;
- $u \sim_\gamma v$.

Consequently, an $A$-generated monoid $M$ belongs to $J_1 \star H$ if and only if $M$ is a morphic image of $A^*/\sim_\gamma$.

**Proof:** Let $u = v$ be an identity on $A$, say $u = a_1 \ldots a_i$ and $v = b_1 \ldots b_j$. Let $N = F_H(A)$ and $M = F_{J_1}(N \times A)$. Consider the left action of $N$ on $M$ defined by $n(n',a) = (nn',a)$ and the associated semidirect product $M \star N$. The embedding of Proposition 2.1 from $F_{J_1 \star H}(A)$ into $M \star N$ that maps $a$ into $((1,a),a)$ maps $u$ into

$$(1) \quad ((1,a_1) + (a_1,a_2) + \cdots + (a_1 \ldots a_{i-1},a_i),a_1 \ldots a_i),$$

and $v$ into

$$(2) \quad ((1,b_1) + (b_1,b_2) + \cdots + (b_1 \ldots b_{j-1},b_j),b_1 \ldots b_j).$$
Denote by $u'$ (respectively $v'$) the first component of (1) (respectively (2)). Then, we have $J_1 \ast H \models u = v$ if and only if $F_{J_1 \ast H}(A) \models u = v$. This is equivalent to the two conditions $F_{J_1}(F_H(A) \times A) \models u' = v'$ and $F_H(A) \models u = v$, or $\alpha(\sigma_\gamma(u)) = \alpha(\sigma_\gamma(v))$ and $u \gamma v$. □

4. A RESULT ON GRAPHS

In the next section, we give a basis of identities for $J_1 \ast H$. In order to do this, we use a result on graphs due to Simon which we state in this section.

A (directed) graph $G$ consists in a set $V$ of vertices, a set $E$ of edges and two mappings $f, g : E \to V$ which to each edge $e$ assigns the start vertex $f(e)$ and the end vertex $g(e)$ of that edge. Two edges $e_1, e_2$ are consecutive if $g(e_1) = f(e_2)$. A path of length $i, i > 0$, is a sequence $e_1 \ldots e_i$ of $i$ consecutive edges. The mappings $f$ and $g$ are extended to mappings $f, g : P \to V$ by letting $f(e_1 \ldots e_i) = f(e_1)$ and $g(e_1 \ldots e_i) = g(e_i)$ ($P$ denotes the set of all paths in $G$). For each vertex $v$ we allow an empty path $1_v$ of length 0 for which $f(1_v) = g(1_v) = v$. A loop about $v$ is a path $x$ such that $f(x) = g(x) = v$.

An equivalence relation $\equiv$ on $P$ is called a congruence if it satisfies the following two conditions:

- If $x \equiv y$, then $x$ and $y$ are coterminal (that is $f(x) = f(y)$ and $g(x) = g(y)$);
- If $x \equiv x', y \equiv y'$ and $g(x) = f(y)$, then $xy \equiv x'y'$.

We agree that each path $1_v$ is congruent only to itself.

**Proposition 4.1** (Simon [8]): Let $\equiv$ be the smallest congruence relation on $P$ satisfying

$$xx \equiv x,$$

$$xy \equiv yx,$$

for any two loops $x, y$ about the same vertex. Then any two coterminal paths traversing the same set of edges (without regard to order and multiplicity) are $\equiv$-equivalent.

The graph $G_\gamma$ of the transducer of the preceding section is useful in the proof of our main result. The set of vertices of $G_\gamma$ is $F_H(A)$, and its set of edges is $F_H(A) \times A$. The start vertex of the edge $(n, a)$ is $n$ and its end vertex is $na$. We use the notation $P_\gamma$ for the set of all paths in $G_\gamma$. To any path

$$x = (n_1, a_1) \ldots (n_i, a_i)$$

in $P_\gamma$, we associate the word $\overline{x} = a_1 \ldots a_i$ in $A^*$. 

vol. 31, n° 3, 1997
If \( u \sim_\gamma v \), then \( \sigma_\gamma(u) \) and \( \sigma_\gamma(v) \) are coterminal paths (with start vertex 1 and end vertex \( \pi_\gamma(u) = \pi_\gamma(v) \)) traversing the same set of edges.

Given a morphism \( \varphi : A^* \to M \) where \( M \) denotes a finite monoid, we can define a congruence \( \cong_\gamma \) on \( P_\gamma \) by \( x \cong_\gamma y \) if \( x \) and \( y \) are coterminal, and if for all paths \( z \) from the vertex 1 to the start vertex of \( x \) and \( y \) we have \( \varphi(zx) = \varphi(zy) \).

5. IDENTITIES FOR \( J_1 * H \)

In this section, we give a basis of identities for \( J_1 * H \).

Let \( A \) be a finite alphabet. Let \( \gamma \) be the congruence generating \( H \) for \( A \) and let \( q \) be a positive integer such that \( u^q \gamma 1 \) for all words \( u \) on \( A \).

**Definition 5.1:** We call a list \( a_1, \ldots, a_i \) of elements of \( A \) \( \gamma \)-circular on \( A \) if \( a_1 \ldots a_i \gamma 1 \) but no nonempty proper prefix of \( a_1 \ldots a_i \) is \( \gamma \)-equivalent to 1. We write \( A_\gamma \) for the set of such \( \gamma \)-circular lists on \( A \).

**Definition 5.2:** We write \( \Sigma_{A, \gamma, q} \) for the set consisting of the identities
\[
(3) \quad x^{2q} = x^q,
\]
\[
(4) \quad x^q y^q = y^q x^q,
\]

Together with all the identities of the form
\[
(5) \quad (y_1 z^q \ldots y_i z^q \ldots y_1 z^q \ldots y_i z^q \ldots y_1) = y_1 z^q \ldots y_i \gamma z^q \ldots y_i \gamma z^q \ldots y_1,
\]
where \( y_1, \ldots, y_i \) is a list in \( A_\gamma \).

The following definition and lemmas will be useful in the proof of Theorem 5.1.

Let us define recursively what we mean by “a \( \gamma \)-word \( w \) on \( A \).

**Definition 5.3:** Basis. The empty word \( 1 \) is a \( \gamma \)-word on \( A \).

Recursive step. If there exists a list \( a_1, \ldots, a_i \) in \( A_\gamma \), and there exist \( v_1, \ldots, v_{i-1} \) which are finite concatenations of \( \gamma \)-words on \( A \) satisfying \( w = a_1 v_1 \ldots a_i v_{i-1} a_i \), then we say that \( w \) is a \( \gamma \)-word on \( A \).

Closure. A word \( w \) is a \( \gamma \)-word on \( A \) only if it can be obtained from the basis by a finite number of applications of the recursive step.
Note that if a word $w$ is a $\gamma$-word on $A$, it is built only from elements of $A$ which build the lists in $A_{\gamma}$.

**Lemma 5.1:** We have $\Sigma_{A,\gamma,q} \vdash (u_1^q \ldots u_i^q)^2 = u_1^q \ldots u_i^q$ and so $\Sigma_{A,\gamma,q} \vdash (u_1^q \ldots u_i^q)^q = u_1^q \ldots u_i^q$.

**Proof:** We have $\Sigma_{A,\gamma,q} \vdash u_1^q \ldots u_i^q = u_1^2 \ldots u_i^2$ since the identity $x^{2q} = x^q$ belongs to $\Sigma_{A,\gamma,q}$, and so $\Sigma_{A,\gamma,q} \vdash u_1^q \ldots u_i^q = (u_1^q \ldots u_i^2)^2$ by using Identity (4) repeatedly. □

**Lemma 5.2:** 1. If $w$ is a $\gamma$-word on $A$, then $\Sigma_{A,\gamma,q} \vdash w^2 = w$ and so $\Sigma_{A,\gamma,q} \vdash w^q = w$;

2. If $w$ and $w'$ are $\gamma$-words on $A$, then $\Sigma_{A,\gamma,q} \vdash ww' = w'w$.

**Proof:** Assertion 1 follows by induction on $w$. Trivially, $\Sigma_{A,\gamma,q} \vdash 1^2 = 1$ and so $\Sigma_{A,\gamma,q} \vdash 1^q = 1$. If $v$ is a finite concatenation of $\gamma$-words on $A$, say $v = u_1 \ldots u_j$, then by using the inductive assumption on $u_1, \ldots, u_j$ as well as Lemma 5.1 we get $\Sigma_{A,\gamma,q} \vdash v^2 = (u_1 \ldots u_j)^2 = (u_1^q \ldots u_j^q)^2 = u_1^q \ldots u_j^q = v$, and so $\Sigma_{A,\gamma,q} \vdash v^q = v$. Now, if there exists a list $a_1, \ldots, a_i$ in $A_{\gamma}$, and there exist $v_1, \ldots, v_{i-1}$ which are finite concatenations of $\gamma$-words on $A$ satisfying $w = a_1v_1 \ldots a_{i-1}v_{i-1}a_i$, then by using an identity of the form (5) we get $\Sigma_{A,\gamma,q} \vdash w^2 = (a_1v_1 \ldots a_{i-1}v_{i-1}a_i)^2 = (a_1v_1^q \ldots a_{i-1}v_{i-1}^q a_i)^2 = a_1v_1^q \ldots a_{i-1}v_{i-1}^q a_i = w$ and so $\Sigma_{A,\gamma,q} \vdash w^q = w$.

Assertion 2 follows from $\Sigma_{A,\gamma,q} \vdash ww' = w^q(w')^q = (w')^qw^q = w'w$. □

**Lemma 5.3:** If $w\gamma_1$, then $\alpha(\sigma_\gamma(u^2)) = \alpha(\sigma_\gamma(u))$. As consequences, $u^{2q} \sim_{\gamma} u^q$ and $u^q v^q \sim_{\gamma} v^q u^q$.

**Proof:** If $w\gamma_1$, then $\sigma_\gamma(u^2) = \sigma_\gamma(u)\sigma_\gamma^u(u) = \sigma_\gamma(u)\sigma_\gamma(u)$ since $\pi_\gamma(u) = 1$. We have $u^q\gamma_1$ and $v^q\gamma_1$, and so $u^q, u^2q, u^q v^q$ and $v^q u^q$ are $\gamma$-equivalent to 1. The equalities $\alpha(\sigma_\gamma(u^{2q})) = \alpha(\sigma_\gamma(u^q))$ and $\alpha(\sigma_\gamma(u^q v^q)) = \alpha(\sigma_\gamma(v^q u^q))$ are easy to check. □

Now, let $r$ be a positive integer and put $A_r = \{x_1, \ldots, x_r\}$. Let $\gamma_r$ be the congruence generating $H$ for $A_r$ and let $q_r$ be a positive integer such that $u^q\gamma_r1$ for all words $u$ on $A_r$.

**Theorem 5.1:** We have $J_1 * H = V(\bigcup_{r \geq 1} \Sigma_{A_r,\gamma_r,q_r})$.

**Proof:** We will show that an $A$-generated monoid $M$ is in $J_1 * H$ if and only if $M \models \Sigma_{A,\gamma,q}$ where $A$ abbreviates $A_r$, $\gamma$ abbreviates $\gamma_r$ and $q$ abbreviates $q_r$. By Lemma 3.2, $A$-generated monoids in $J_1 * H$ satisfy identities $u = v$.
where $u \sim_\gamma v$ (that is $\alpha(\sigma_\gamma(u)) = \alpha(\sigma_\gamma(v))$ and $u \gamma v$). Lemma 5.3 implies that $x^{2q} \sim_\gamma x^q$ and $x^q y^q \sim_\gamma y^q x^q$. We also have $x^2 \sim_\gamma x$ for all the identities $x^2 = x$ of the form (5). To see this, put $x = y_1 \ldots y_i z_{i-1}^{-1} y_i$ with $y_1, \ldots, y_i$ a list in $A_\gamma$. Since $x$ is $\gamma$-equivalent to 1, we get $x^2 \gamma x$. The equality $\alpha(\sigma_\gamma(x^2)) = \alpha(\sigma_\gamma(x))$ follows from Lemma 5.3.

Conversely, let $\varphi : A^* \to M$ be a surjective morphism satisfying $\varphi(u) = \varphi(v)$ for every identity $u = v$ in $\Sigma_{A, \gamma, q}$. We also denote by $\varphi$ the (nuclear) congruence on $A^*$ associated with $\varphi$ and defined by $u \varphi v$ if and only if $\varphi(u) = \varphi(v)$. We show the inclusion $\sim_\gamma \subseteq \varphi$ which yields $M = A^*/\varphi$ is a morphic image of $A^*/\sim_\gamma$. The membership of $M$ to $J_1 * H$ follows by Lemma 3.2.

We consider the graph $G_\gamma$ and the congruence relation $\equiv_\gamma$ on its set of paths $P_\gamma$ defined at the end of Section 4. Let $x$ and $y$ be two loops about the same vertex $\pi_\gamma(w)$, or

$$x = (\pi_\gamma(w), a_1) \ldots (\pi_\gamma(w a_1 \ldots a_{i-1}), a_i),$$

$$y = (\pi_\gamma(w), b_1) \ldots (\pi_\gamma(w b_1 \ldots b_{j-1}), b_j),$$

where $w a_1 \ldots a_i \gamma w \gamma w b_1 \ldots b_j$. We show the following two claims: Claim 1 or $xx \equiv_\gamma x$, and Claim 2 or $xy \equiv_\gamma yx$. Now if $u \sim_\gamma v$, then $\sigma_\gamma(u)$ and $\sigma_\gamma(v)$ are two coterminial paths traversing the same set of edges (the start vertex of $\sigma_\gamma(u)$ and $\sigma_\gamma(v)$ is 1 and their end vertex is $\pi_\gamma(u) = \pi_\gamma(v)$). Hence, by Proposition 4.1, $\sigma_\gamma(u) \equiv_\gamma \sigma_\gamma(v)$. Therefore, $\varphi(\sigma_\gamma(u)) = \varphi(\sigma_\gamma(v))$ or $\varphi(u) = \varphi(v)$ and the inclusion $\sim_\gamma \subseteq \varphi$ follows.

Let us now prove Claim 1 and Claim 2. Since $wa_1 \ldots a_i \gamma w$ and $wb_1 \ldots b_j \gamma w$, we have $\bar{x} = a_1 \ldots a_i \gamma 1$ and $\bar{y} = b_1 \ldots b_j \gamma 1$ since $H$ is a pseudovariety of groups.

**Proof of Claim 1**: The condition $xx \equiv_\gamma x$ follows by showing that $\varphi(\bar{x} \bar{x}) = \varphi(\bar{x} \bar{x})$ for all paths $z$ from the vertex 1 to the start vertex of $x$. Here we can show that $\varphi(\bar{x} \bar{x}) = \varphi(\bar{x})$ (and therefore $\varphi(\bar{x}^q) = \varphi(\bar{x})$). The word $\bar{x}$ has the property $\mathcal{P}$ that "it is $\gamma$-equivalent to 1". The word $\bar{x}$ can be factorized as follows: let $u_1$ be the smallest nonempty prefix of $\bar{x}$ with Property $\mathcal{P}$; let $u_2$ be the smallest nonempty prefix of $\bar{x} \setminus u_1$ with Property $\mathcal{P}$; \ldots. So $\bar{x}$ is a concatenation of factors $u_1 \ldots u_n$ with Property $\mathcal{P}$. Since no nonempty proper prefix of $u_1$ has Property $\mathcal{P}$, let $c_1 v_1$ be the shortest prefix of $u_1$ such that $\pi_\gamma(c_1 v_1) = \pi_\gamma(c_1)$; \ldots let $c_{\ell-1} v_{\ell-1}$ be the shortest prefix of $u_1 \setminus c_1 v_1 \ldots c_{\ell-2} v_{\ell-2}$ such that $\pi_\gamma(c_1 v_1 \ldots c_{\ell-2} v_{\ell-2} c_{\ell-1}) = \pi_\gamma(c_1 v_1 \ldots c_{\ell-2} v_{\ell-2} c_{\ell-1})$; and
let \( c_\ell = u_1 \setminus c_1 v_1 \ldots c_{\ell-1} v_{\ell-1} \) satisfying \( \pi_\gamma(c_1 v_1 \ldots c_{\ell-1} v_{\ell-1} c_\ell) = \pi_\gamma(1) \).

So \( u_1 = c_1 v_1 \ldots c_{\ell-1} v_{\ell-1} c_\ell \) where \( c_1, \ldots, c_\ell \in A_\gamma \) and where the \( v \)-factors have Property \( P \) (similar statements hold for \( u_2, \ldots, u_n \)). Since the \( v \)-factors have Property \( P \), they can be factorized as above and the process can be repeated. Factors in \( \overline{x} \) are hence \( \gamma \)-words on \( A \). We have \( \varphi(u_1) = \varphi(u_1^q), \ldots, \varphi(u_n) = \varphi(u_n^q) \) (as in Lemma 5.2). Therefore \( \varphi(\overline{x}) = \varphi(u_1 \ldots u_n) = \varphi(u_1^q \ldots u_n^q) = \varphi((u_1^q \ldots u_n^q)^2) \) (as in Lemma 5.1) \( \varphi(\overline{x}^2) = \varphi(\overline{x} \overline{x}). \)

**Proof of Claim 2:** The condition \( xy \cong \gamma yx \) follows from \( \varphi(\overline{x} \overline{y}) = \varphi(\overline{x} \overline{y}) = \varphi(\overline{x}) \varphi(\overline{y}) = \varphi(\overline{x}^q) \varphi(\overline{y}^q) = \varphi(\overline{x}^q \overline{y}^q) = \varphi(\overline{y} \overline{x}) \) (using Identity (4)). \( \square \)

6. IDENTITIES FOR \( J_1 * G_p \)

In this section, we give a sequence of sets of identities ultimately defining \( J_1 * G_p \).

Let \( A \) be a finite alphabet and let \( u, w \in A^* \) with \( u = a_1 \ldots a_t \). The binomial coefficient \( \binom{w}{u} \) is defined as the number of distinct factorizations of the form

\[ w = w_0 a_1 v_1 \ldots a_t v_t \]

with \( w_0, \ldots, v_t \in A^* \). Thus the binomial coefficient counts the number of ways in which \( u \) is a subword of \( w \). We adopt the convention that \( \binom{w}{1} = 1 \).

Let \( a, b \in A \) and \( u, w, w' \in A^* \). The following formulas are easily verified:

- \( \binom{a^j}{a} = \binom{j}{j} \) where \( i \geq j \);
- \( \binom{1}{a} = \begin{cases} 1, & \text{if } u = 1, \\ 0, & \text{otherwise}; \end{cases} \)
- \( \binom{a^u}{u} = \begin{cases} 1, & \text{if } u = 1 \text{ or } u = a, \\ 0, & \text{otherwise}; \end{cases} \)
- \( \binom{w^a}{u} = \binom{w}{u} + \delta_{a,b} \binom{w}{u} \) where \( \delta_{a,b} = \begin{cases} 1, & \text{if } a = b, \\ 0, & \text{otherwise}; \end{cases} \)
- \( \binom{w w'}{u} = \sum_{u = u v'} \binom{w}{v} \binom{w'}{v'} \).

Given a word \( u \) on \( A \), we define on \( A^* \) the equivalence relation \( \gamma_{p,u} \) by \( w \gamma_{p,u} w' \) if and only if \( \binom{w}{v} \equiv \binom{w'}{v} \mod p \) whenever \( u \in A^* v A^* \).

Now, given an integer \( k \geq 0 \), we define on \( A^* \) the equivalence relation \( \gamma_{p,k} \) by \( \gamma_{p,k} = \bigcap_{|u|=k} \gamma_{p,u} \). Thus \( w \gamma_{p,k} w' \) if and only if \( \binom{w}{v} \equiv \binom{w'}{v} \mod p \) whenever \( |v| \leq k \).

Note that for all \( w, w' \in A^* \) we have \( w \gamma_{p,0} w' \).
Lemma 6.1 (Eilenberg [8]): The equivalence relations \( \gamma_{p,u} \) and \( \gamma_{p,k} \) are congruences of finite index on \( A^* \).

Lemma 6.2 (Eilenberg [8]): Let \( k \) be a positive integer and \( u \in A^* \). If \( w \in A^* \), then \( w^{p^k} \gamma_{p,u} 1 \) and \( w^{p^k} \gamma_{p,k} 1 \).

Proof: If \( w \in A^* \), then the following conditions are equivalent:

- \( w \gamma_{p,k} 1; \)
- \( (w_u) \equiv 0 \mod p \) whenever \( 0 < |u| \leq k \).

We show the \( \gamma_{p,k} \)-equivalence of \( w^{p^k} \) and 1. For \( k = 1 \), the result holds trivially. We proceed by induction and assume \( 0 < |v| \leq k + 1 \). Then

\[
(w^{p^{k+1}}_v) = \sum (w^{p^k}_{v_1}) \ldots (w^{p^k}_{v_p}),
\]

where the summation extends over all factorizations \( v = v_1 \ldots v_p \) of \( v \). If for some \( 1 \leq i \leq p \) we have \( 0 < |v_i| < k + 1 \), then by the inductive assumption \( (w^{p^k}_{v_i}) \equiv 0 \mod p \) and the summand may be omitted. There remain summands with \( v_i = v, v_j = 1 \) for \( j \neq i \). Each such summand yields \( (w^{p^k}_v) \) and there are exactly \( p \) such summands. Thus \( (w^{p^{k+1}}_v) \equiv 0 \mod p \) as required.

The quotients \( A^*/\gamma_{p,u} \) and \( A^*/\gamma_{p,k} \) are finite monoids by Lemma 6.1. Lemma 6.2 implies that \( A^*/\gamma_{p,u} \) satisfies the identity \( x^{p^{|u|}} = 1 \) and \( A^*/\gamma_{p,k} \) the identity \( x^{p^k} = 1 \). Note that \( A^*/\gamma_{p,0} \) is the trivial group. If \( A = \{a_1, \ldots, a_r\} \), \( A^*/\gamma_{p,1} \) is isomorphic to the set of all words of the form \( a_1^{e_1} \cdots a_r^{e_r} \) with \( 0 \leq e_i < p \) multiplying two such words through the addition of the respective exponents.

We now describe the \(*\)-variety \( G_p \) of sets defined by the pseudovariety \( G_p \).

Lemma 6.3 (Eilenberg [8]): • The pseudovariety \( G_p \) is generated by the groups \( A^*/\gamma_{p,k} \) for all integers \( k \geq 0 \) and all finite alphabets \( A \), or by the groups \( A^*/\gamma_{p,u} \) for all elements \( u \in A^* \) and all finite alphabets \( A \).

- \( A^* G_p \) is the boolean closure of the sets

\[
\{w \in A^* \mid (w_u) \equiv i \mod p\}, \ u \in A^*, \ 0 \leq i < p.
\]

Let \( k \) be a nonnegative integer and define the pseudovariety \( H_{p,k} \) as the locally finite pseudovariety of groups generated by \( A^*/\gamma_{p,k} \) for all finite alphabets \( A \). The \(*\)-variety \( A^* H_{p,k} \) is then the boolean closure of the sets

\[
\{w \in A^* \mid (w_u) \equiv i \mod p\}, \ u \in A^* \text{ with } |u| \leq k, \ 0 \leq i < p.
\]
The pseudovariety $H_{p,0}$ is the trivial pseudovariety $I = V(x = 1)$. Since $I$ is the unit element for the semidirect product operation on pseudovarieties of monoids, we have $J_1 * H_{p,0} = J_1 = V(x^2 = x, xy = yx)$. 

Now, let $k$ be a positive integer. A list $a_1, \ldots, a_i$ of elements of $A$ is $\gamma_{p,k}$-circular on $A$ if $(a_1 \cdots a_i) \equiv 0 \mod p$ whenever $0 < |v| \leq k$, but no nonempty proper prefix $w$ of $a_1 \cdots a_i$ satisfies $(w) \equiv 0 \mod p$ for every $0 < |v| \leq k$. For example, $a, b, b, a, a, b, b, a$ is a list in $\{a, b\}_{\gamma_{2,2}}$.

If $k$ and $r$ are positive integers, we write $\Sigma^r_{p,k}$ for the set consisting of the identities

\begin{align*}
(6) & \quad x^{2p^k} = x^{p^k}, \\
(7) & \quad x^{p^k} y^{p^k} = y^{p^k} x^{p^k},
\end{align*}

together with all the identities of the form

\begin{align*}
(8) & \quad (y_1 z_1^{p^k} \cdots y_{i-1} z_{i-1}^{p^k} y_i)^2 = y_1 z_1^{p^k} \cdots y_{i-1} z_{i-1}^{p^k} y_i,
\end{align*}

where $y_1, \ldots, y_i$ is a list in $\{x_1, \ldots, x_r\}_{\gamma_{p,k}}$. We write $\Sigma_{p,k}$ for $\bigcup_{r \geq 1} \Sigma^r_{p,k}$.

Continuing with the above example, the identity $x^2 = x$ where

\begin{align*}
x = x_1 z_1^{2^2} x_2 z_2^{2^2} x_2 z_2^{2^2} x_1 z_1^{2^2} x_1 z_1^{2^2} x_2 z_2^{2^2} x_2 z_2^{2^2} x_1,
\end{align*}

belongs to $\Sigma^2_{2,2}$.

For $r \geq 1$, $\Sigma^r_{p,k} \subseteq \Sigma^{r+1}_{p,k}$. This follows from the fact that if $A \subseteq B$, then $A_{\gamma_{p,k}} \subseteq B_{\gamma_{p,k}}$.

**Corollary 6.1**: The pseudovariety $J_1 * G_p$ is ultimately defined by $\Sigma_{p,k}$, $k \geq 1$ or a monoid is in $J_1 * G_p$ if and only if it satisfies $\Sigma_{p,k}$ for all $k$ sufficiently large.

**Proof**: By Theorem 5.1, the pseudovariety $J_1 * H_{p,k}$ is defined by $\Sigma_{p,k}$. Now, the semidirect product operation on pseudovarieties commutes with directed unions [3]. We get $J_1 * G_p = J_1 * \bigcup_{k \geq 0} H_{p,k} = \bigcup_{k \geq 0} J_1 * H_{p,k} = \bigcup_{k \geq 1} J_1 * H_{p,k}$ and the result follows. 

**REFERENCES**


vol. 31, n° 3, 1997