On Pseudovarieties

SAMUEL EILENBERG AND M. P. SCHÜTZENBERGER

Columbia University and University of Paris VII

Reprinted from ADVANCES IN MATHEMATICS
All Rights Reserved by Academic Press, New York and London

Vol. 19, No. 3, March 1976
Printed in Belgium

Reprinted from ADVANCES IN MATHEMATICS
All Rights Reserved by Academic Press, New York and London

Vol. 19, No. 3, March 1976
Printed in Belgium

On Pseudovarieties

SAMUEL EILENBERG* AND M. P. SCHÜTZENBERGER

Columbia University and University of Paris VII

DEDICATED TO GARRETT BIRKHOFF

Birkhoff's Theorem [1] asserts that a family of algebras is an equational variety if and only if the family is closed under the operations of passing to subalgebras and quotient algebras and also under arbitrary direct products. The objective of this paper is to study what happens to this notion and the theorem above if one restricts ones attention to finite algebras only. This is motivated by applications to the theory of automata.

In the body of the paper, we shall only consider monoids. At the end, we shall remark how the results can be extended to more general species of algebras.

A family $\mathbf{V}$ of finite monoids is called a *pseudovariety* if the following conditions hold

(1) If $S \in \mathbf{V}$ and T is a submonoid of S, then $T \in \mathbf{V}$.

(2) If $S \in \mathbf{V}$ and T is a homomorphic image of S, then $T \in \mathbf{V}$.

(3) If $S, T \in \mathbf{V}$, then $S \times T \in \mathbf{V}$.

There are two points in which this definition differs from that of a (Birkhoffian) variety. One is that all the monoids in $\mathbf{V}$ are assumed to be *finite*. The second one (implied by the first) is that $\mathbf{V}$ is closed only under finite direct products. For example finite groups form a pseudovariety, but groups do not form a variety of monoids. Indeed, a submonoid of an (infinite) group need not be a group. It should however be noted that a finite monoid S is a group if and only if, for all n sufficiently large, and for all $x \in S$, the equation

$$x^n = 1$$

* Research partially supported by NSF Grant DCR 72-03703 A01.

holds, where $\bar{n}$ is the least common multiple of all the integers $1 < i \leqslant n$. The objective of this paper is to show that such a phenomenon holds for all pseudovarieties.

Let Ξ^* be the free monoid generated by the infinite sequence of letters $x_1, \ldots, x_n, \ldots$ and let $u, v \in \Xi^*$. We shall say that a monoid S *satisfies* (u, v) (or that the equation $u = v$ *holds* in S) if $u\varphi = v\varphi$ for every morphism $\varphi: \Xi^* \to S$. Finite monoids satisfying (u, v) clearly from a pseudovariety that we shall denote by $\mathbf{V}(u, v)$.

Given a sequence of pairs

$$(u_i, v_i) \in \Xi^* \times \Xi^*, \qquad i \geqslant 1,$$

we may consider two pseudovarieties

$$\mathbf{V}' = \bigcap_{i=1}^{\infty} \mathbf{V}(u_i, v_i),$$

$$\mathbf{V} = \bigcup_{k=1}^{\infty} \bigcap_{i=k}^{\infty} \mathbf{V}(u_i, v_i).$$

A (finite) monoid is in $\mathbf{V}'$ if it satisfies all of the equations $u_i = v_i$, while it is in $\mathbf{V}$ if it satisfies the equations $u_i = v_i$ for all i sufficiently large. We shall say that $\mathbf{V}'$ is *defined* by the equations $u_i = v_i$, and that $\mathbf{V}$ is *ultimately defined* by the equations $u_i = v_i$.

Our main result is

THEOREM 1. *Each nonempty pseudovariety* $\mathbf{V}$ *is ultimately defined by a sequence of equations.*

We denote by Ξ_n^* the submonoid of Ξ^* generated by the letters $x_1, \ldots, x_n$. In Ξ_n^*, we shall consider congruences. Such a congruence $\sim$ in Ξ_n^* is said to be finite provided the quotient monoid $\Xi_n^*/\sim$ is finite. An important fact in the proof of Theorem 1 is

PROPOSITION 2. *A finite congruence $\sim$ in Ξ_n^* is finitely generated, i.e., there exists a finite set $W \subset \Xi_n^* \times \Xi_n^*$ such that $u \sim v$ for all $(u, v) \in W$, and such that $\sim$ is the smallest congruence with this property.*

Proof. Since the congruence $\sim$ is finite, there exists an integer $k > 0$ such that each congruence class contains an element w with length $|w| < k$. Define

$$W = \{(u, v) \mid u \sim v, |u| \leqslant k, |v| < k\}.$$

Clearly, card $W < (1 + n)^{2k-1}$. Let $\equiv$ be the congruence generated by W. Clearly, $u \equiv v$ implies $u \sim v$. To prove the opposite implication, we need the following assertion

(4) For each $w \in \Xi_n^*$, there exists $w' \in \Xi_n^*$ such that $| w' | < k$ and $w \equiv w'$.

We prove this by induction with respect to $| w |$. If $| w | < k$, there is nothing to prove since $(w, w) \in W$. Assume now that $l > k$ and that (4) holds for all w with $| w | < l$. Consider $w \in \Xi_n^*$, $| w | = l$. Then, $w = u\sigma$ with $| u | = l - 1$. Consequently $u \equiv u'$ for some u' with $| u' | < k$. This implies $w \equiv u'\sigma$. Since $| u'\sigma | = k$, the definition of W implies that $(u'\sigma, w') \in W$ for some w' such that $| w' | < k$. It follows that $w \equiv w'$ as required.

Now, assume $u \sim v$. By (4) we have $u \equiv u'$ and $v \equiv v'$ with $| u' | < k$, $| v' | < k$. Since $u' \sim v'$, it follows that $(u', v') \in W$ and thus, $u' \equiv v'$. Consequently, $u \equiv v$. This proves that $\sim$ and $\equiv$ coincide and thus, $\sim$ is finitely generated.

Having proved Proposition 2, we now proceed with the proof of Theorem 1.

We first construct a sequence

$$S_1, S_2, \ldots, S_n, \ldots,$$

in $\mathbf{V}$ with the following two properties

(5) S_n is isomorphic to a quotient of S_{n+1}.

(6) If $S \in \mathbf{V}$, then S is isomorphic to a quotient of S_n for some $n \geqslant 1$.

To construct such a sequence, we write a sequence $T_1, T_2, \ldots, T_n, \ldots,$ which contains all the elements of $\mathbf{V}$ up to an isomorphism, and then define $S_n = T_1 \times \cdots \times T_n$.

For each $n \geqslant 1$, we define the congruence $\sim_n$ in Ξ_n^* as follows: $u \sim_n v$ iff $u\varphi = v\varphi$ for all morphisms $\varphi: \Xi_n^* \to S_n$. Consider the quotient monoid V_n^3 of Ξ_n^* by the congruence $\sim_n$. The following facts are clear

(7) V_n is isomorphic to a submonoid of some finite product of S_n with itself.

This implies

(8) $V_n \in \mathbf{V}$.

Since V_n is finite, Proposition 2 may be applied to the congruence

$\sim_n$, yielding a finite set $W_n \subset \Xi_n^* \times \Xi_n^*$, such that $\sim_n$ is generated by W_n. Since Ξ_n^* is a subset of Ξ^*, we obtain the countable set

$$W = \bigcup_{n=1}^{\infty} W_n$$

in $\Xi^* \times \Xi^*$. We assert that W ultimately defines $\mathbf{V}$.

First, assume that $S \in \mathbf{V}$. Since S is isomorphic to a quotient of S_n for some $n \geqslant 1$, and since S_n satisfies the equations W_n, it follows that S satisfies the equations W_n. However, S_n is isomorphic to a quotient of S_{n+k} for all $k \geqslant 0$ and thus, S also satisfies all the equations W_{n+k} for all $k \geqslant 0$. Thus, S satisfies all but a finite number of equations in W.

Conversely, assume that S is a finite monoid satisfying all but a finite number of equations in W. Choose $n \geqslant 1$ with the following two properties

(9) $n \geqslant \operatorname{card} S$,

(10) S satisfies the equations W_n.

Let

$$\varphi\colon \Xi_n^* \to S,$$

be a surjective morphism. If $(u, v) \in W_n$, then $u\varphi = v\varphi$ since S satisfies the equation $u = v$. Since the pairs (u, v) in W_n generate the congruence $\sim_n$, it follows that $u \sim_n v$ implies $u\varphi = v\varphi$. This implies that φ admits a factorization

$$\Xi_n^* \longrightarrow V_n \xrightarrow{\psi} S,$$

and that ψ is a surjective morphism. Since $V_n \in \mathbf{V}$, it follows that $S \in \mathbf{V}$· This concludes the proof of Theorem 1.

A pseudovariety $\mathbf{V}$ is said to be *equational* if it is defined by a family of equations. This holds if and only if $\mathbf{V}$ is the class of all finite monoids in some (Birkhoffian) variety of monoids. However, two distinct varieties may yield the same pseudovariety.

An immediate consequence of Theorem 1 is

COROLLARY 3. *Each pseudovariety is the union of an ascending sequence of equational pseudovarieties.*

A pseudovariety $\mathbf{V}$ is said to be *finitely generated*, if there exists a finite sequence of monoids $M_1, \ldots, M_k$ such that $\mathbf{V}$ is the smallest pseudovariety containing $M_1, \ldots, M_k$. Replacing this sequence by the single monoid $M = M_1 \times \cdots \times M_k$, shows that each finitely generated pseudovariety is generated by a single monoid M. A consequence of Corollary 3 is

Corollary 4. *Each finitely generated pseudovariety is equational.*

The remarks above lead in a natural way to consider the following two properties of a finite monoid M

(11) The variety generated by M is defined by a finite number of equations.

(12) The pseudovariety generated by M is defined by a finite number of equations.

The implication (11) ⇒ (12) is clear. Whether the implication (12) ⇒ (11) holds is an open question. Oates and Powell [3] have shown that (11) holds for any finite group. This easily implies (12) for any finite group. Perkins [4] has constructed a monoid containing six elements for which (11) fails. It is an open question whether (12) holds for this monoid. Perkins' monoid may be described as the monoid of all partial functions $f\colon \{0, 1\} \rightarrow \{0, 1\}$, but excluding the two constant functions and the function that interchanges 0 and 1.

Although we have limited our attention to monoids, the entire development can be carried out for any algebraic theory based on a finite number of finitary operations. The role of Ξ^* and $\Xi_n{}^*$ is then taken over by the free algebras generated by $x_1, \ldots, x_n, \ldots,$ and by $x_1, \ldots, x_n$. For $u \in \Xi^*$ or $u \in \Xi_n{}^*$, the integer $|u|$ must be defined in such a way that the proof of Proposition 2 remains valid. A fact needed in this proof is the finiteness of the sets $\{u \mid u \in \Xi_n{}^*, |u| \leqslant k\}$. This follows from the assumption that there is only a finite number of basic operations.

Pseudovarieties of monoids and of semigroups have applications in the theory of automata. The interested reader is referrred to Eilenberg [2], where the ultimate equations of many interesting pseudovarieties are derived.

In connection with pseudovarieties of semigroups, the following interesting fact should be noted. Finite groups form a pseudovariety **G** of monoids. However, **G** is not a pseudovariety of semigroups because it does not contain the empty semigroup. If, however, the empty semigroup is adjoined to **G**, a pseudovariety **G**′ of semigroups is obtained. Its ultimate equations are obtained by replacing each equation $x^{n} = 1$

used to ultimately define **G** by the pair of equations $x^{\bar{n}}y = y = yx^{\bar{n}}$. These new equations ultimately define **G**′ as a pseudovariety of semigroups, and **G** as a pseudovariety of monoids. This method of eliminating the unit element is quite general.

References

1. Garrett Birkhoff, On the structure of abstract algebras, *Proc. Cambridge Phil. Soc.* 31 (1935), 433–454.
2. Samuel Eilenberg, "Automata, Languages and Machines, Vol. B," Academic Press, New York, 1976.
3. Sheila Oates and M. B. Powell, Identical relations in finite groups, *J. Algebra* 1 (1964), 11–39.
4. Peter Perkins, Bases for equational theories of semigroups, *J. Algebra* 11 (1968), 298–314.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.