FINITE MODELS OF IDENTITIES

SHERMAN K. STEIN¹

1. Introduction. If Φ is a set of identities on a groupoid (i.e. a binary function) then $V(\Phi)$ denotes the class of groupoids satisfying Φ , i.e. the models of Φ . The variety, $V(\Phi)$, is clearly closed under homomorphic image, direct product, and subgroupoid. The set of identities which are formal consequences of Φ , we denote Φ' ; clearly $\Phi'' = \Phi' \supset \Phi$. In (1) Birkhoff proved that any class of groupoids, closed under those three operations, is $V(\Phi)$ for some Φ . We shall examine the finite models of some specific Φ to answer these questions: Is a variety determined by its finite members? If every finite member of a variety is a quasigroup, is every member? Can two identities have the same finite models and yet not determine the same variety?

2. Varieties having exactly one finite member. Every variety contains the groupoid with one element. At the opposite extreme to varieties determined by their finite members are those which have only one finite member, the trivial groupoid. That there are such varieties is shown by the following theorem which utilizes a construction of Kalicki [2]. We shall need this number-theoretic

LEMMA 2.1. *There exist subsets M and N of $J = \{1, 2, \dots\}$ such that $M \cap N = \emptyset$, $M \cup N = J$ and neither M nor N contains an infinite arithmetic progression.*

Though this lemma is probably part of the literature related to van der Waerden's well-known theorem on arithmetic progressions, the construction following is included for convenience.

Index the set of infinite arithmetical progressions $A_1, A_2, A_3, \dots$. We shall define two increasing sequences in J , $m_1, m_2, \dots$ and $n_1, n_2, \dots$. Let m_1 be any element of A_1 and n_1 be any larger element of A_1 . Having defined $m_1, \dots, m_k, n_1, \dots, n_k$, define m_{k+1} as any element of A_{k+1} greater than n_k and n_{k+1} as any element in A_{k+1} greater than m_{k+1} . Let $M' = \bigcup_k \{m_k\}$, $N' = \bigcup_k \{n_k\}$ and M and N be disjoint sets, $M \supset M'$, $N \supset N'$, $M \cup N = J$. These M and N satisfy the conditions of Lemma 2.1.

THEOREM 2.2. *There exists a nontrivial variety having only one finite member.*

Received by the editors February 16, 1962.

¹ This research was supported by the Air Force Office of Scientific Research.

PROOF. Let M and N be as in Lemma 2.1 with $1 \in M$. For convenience, if U is a term $S(U)$ denotes the term (UU) ; $S^k(U)$ denotes the term obtained by applying S k times.

Let Φ consist of the identities: $XX \cdot X = YY \cdot Y$, $S^m(X) \cdot X = XX \cdot X$ if $m \in M$, $S^n(X) \cdot X = X$ if $n \in N$. That $V(\Phi)$ is not trivial follows from the fact that the following groupoid " $\circ$ " defined on J is a Φ -groupoid. Let $(i+1) \circ i = 1$ for all $i \in J$, $(i+m) \circ i = 1$ if $m \in M$, $(i+n) \circ i = i$ if $n \in N$, $i \circ i = i+1$ for all $i \in J$ and $i \circ j = j \circ i$ if $j > i$. (Kalicki constructed this Φ for any partition M, N of J).

Now we show that any finite Φ -groupoid satisfies the identity $X = Y$. Let A be a finite Φ -groupoid and $s: A \rightarrow A$ be defined by $s(x) = xx$. Since A is finite there are distinct integers a and b , $a > b$, such that $s^a = s^b$.

Let us assume that $b \in M$. Calling $a - b = c$ we have $s^c s^b = s^b$. Since M contains no infinite arithmetic progression there is an integer k such that $b + kc \in N$. Thus

$$(s^{b+kc}x) \circ x = x \quad \text{for all } x \in A.$$

On the other hand, since $s^c s^b = s^b$ we have

$$(s^{b+kc}x) \circ x = (s^b x) \circ x = xx \cdot x.$$

Thus A satisfies the identity $XX \cdot X = X$. But A satisfies $XX \cdot X = YY \cdot Y$ and $YY \cdot Y = Y$. Thus A satisfies $X = Y$ and the theorem is proved.

Theorem 2.2 could be derived from Kalicki's general result [2] in a nonconstructive manner as is shown by

THEOREM 2.3. *If $V = \{V_a: a \in A\}$ is an uncountable set of varieties, each pair of which shares only the trivial groupoid, then there is a V_a having only one finite member.*

Theorem 2.3 is a consequence of the fact that the number of finite groupoids is denumerable.

A similar theorem holds for complete sets of identities. (Φ is a complete set of identities if $\psi \supset \Phi$ implies $\psi' = \Phi'$ or $\psi' = \{X = Y\}'$, but $\Phi' \neq \{X = Y\}'$.)

THEOREM 2.4. *If $\{\Phi_a: a \in A\}$ is an uncountable set of distinct complete families of identities then there is a $V(\Phi_a)$ having only one finite member.*

PROOF. In [3] Scott proved that if A is a finite groupoid then $\Phi(A)$ is contained in only a finite number of complete families. From this and the denumerability of the set of finite groupoids the theorem follows.

3. Translation identities. The variety defined in §2 requires Φ to be infinite and has but one finite member. We now show that with Φ consisting of just one identity varieties can be constructed which, though possessing an infinite set of finite members, are not determined by them.

If instead of varieties of groupoids we considered varieties consisting of two unary functions, f, g , then it would be a simple matter to construct such a Φ . Indeed, consider the variety with two unary functions, f and g , satisfying the identity $fg(x) = x$.

In any finite model of this identity f and g are bijections inverse to each other and hence satisfy the identity $g(f(x)) = x$. For infinite models this is not necessarily the case. This variety has nontrivial finite members but is not determined by them.

To show that the same phenomenon occurs in groupoids with one binary function we consider a special type of identity obtained by equating compositions of translations. If A is a groupoid and $a \in A$ then denote by $L_a: A \rightarrow A$ left translation by a and by $R_a: A \rightarrow A$ right translation. Any identity $U = V$ such that some letter appears exactly once in U and once in V can be expressed as the equality of composition of translations. For example, associativity, $X \cdot YZ = XY \cdot Z$ is expressible as $L_x R_z = R_z L_x$ or $L_{xy} = L_x L_y$, or $R_{yz} = R_z R_y$. Commutativity is $R_x = L_x$. The constant groupoids are described by $R_x = L_y$.

Moreover, some well known conditions imposed on quasigroups are conjugate to translation identities. For example, in [4] Artzy examined quasigroups A satisfying the inverse property: for each $x \in Q$ there is $x' \in Q$ so that $xy \cdot x' = y$. Thus, $xu = p$, $px' = u$, $xv = q$ imply $qx' = v$. Conjugating (see [5]) this predicate by (2, 3) we obtain

$$xp = u, \quad pu = x', \quad xq = v \quad \text{imply} \quad qv = x'.$$

That is,

$$p \cdot xp = x' \quad \text{implies} \quad q \cdot xq = x',$$

or simply

$$L_p R_p = L_q R_q.$$

If furthermore we impose $(x')' = x$ then the (2, 3)-conjugate of Artzy's inverse property becomes $L_a R_a L_b R_b = I$. It is easy to show that any groupoid satisfying $L_a R_a L_b R_b = I$ is a quasigroup.

We shall tacitly assume the subscripts are all the same single letter in what follows. For example, " $L = R$ " is short for " $L_a = R_a$ for all $a \in A$ ", the condition that A be commutative. An equality of the form $M = N$, where M and N are strings of L 's and R 's or just I ,

the identity function, thus corresponds to an identity on A and will be called an identity.

The identity $LL=I$ is the left law of keys. $LR=RL$ is the identity $A \cdot BA = AB \cdot A$, a weak form of associativity. $LL=R$ arose in the study of orthogonal quasigroups [5, p. 246]. $L=I$ or $R=I$ define the singular semigroups.

THEOREM 3.1. *Any model M of $LR=I$ is a quasigroup satisfying $RL=I$.*

PROOF. M satisfies the identity $A \cdot BA = B$; we wish to show that M satisfies $AB \cdot A = B$. Any model of $A \cdot BA = B$ is a model of $AB \cdot A = AB(B \cdot AB)$ and $AB(B \cdot AB) = B$. Thus M satisfies $AB \cdot A = B$.

From the two relations $LR=I$ and $RL=I$ it follows that both R and L are bijections, that is, M is a quasigroup. This ends the proof.

THEOREM 3.2. *If S is a sequence of L 's and R 's containing at least one R , then any model of $LSL=I$ is a quasigroup.*

PROOF. Multiplying both sides of $LSL=I$ by LS we obtain $LSLSL=LS$ and hence $SL=LS$. Replacement of LS in LSL by SL yields $SLL=I$. If S is of the form L^nRS' , with S' some sequence of L 's and R 's, then $n+1$ applications of this process produces an equation $RS''L^nL=I$, where S'' is some sequence of L 's and R 's.

Thus R is a surjection. In a similar way it can be shown that R is an injection, hence bijection. The identity $LSL=I$ shows L is a bijection. Thus A is a quasigroup.

THEOREM 3.3. *If S is a sequence of L 's and R 's, then any finite model of $LSR=I$ is a quasigroup satisfying an identity of the form $RS'L=I$, where S' is a sequence of L 's and R 's depending only on S .*

PROOF. Since $LSR=I$ it follows that L is a surjection and R an injection. By finiteness, L and R are bijections. Thus each finite model is a quasigroup.

If S is void Theorem 3.1 implies $RL=I$. Assume that S is not void and hence² is of the form L^nT , with T a sequence of L 's and R 's not beginning with L and $n>0$. If T is void we have $LL^nR=I$. Thus L^{n+1} and R , being inverse, commute, that is, $RLL^n=I$, or $RL^nL=I$. So the theorem is proved for void T .

If T is not void it is of the form RT' , with T' a sequence of R 's and L 's. Then we have $LL^nRT'R=I$. Thus L^{n+1} and $RT'R$ commute, that is, $RT'RLL^n=I$ or $RT'RL^nL=I$. Thus the theorem holds for nonvoid T also.

² A similar argument holds for the case in which S is of the form R^nT .

Theorem 3.3 suggests that there exist identities γ and δ on groupoids such that every finite γ -model is a δ -model even though δ is not a consequence of γ . It also suggests that there are identities γ all of whose finite models are quasigroups though not all γ -models are quasigroups. In fact we shall prove

THEOREM 3.4. *There is a model of the identity $LRLR=I$ which is not a model of $RLRL=I$. Equivalently, there is a model of $LRLR=I$ which is not a quasigroup.*

Theorem 3.4 shows us that there are two distinct varieties, each defined by a single identity, whose finite members coincide. Moreover these varieties have many finite members, for example the groupoids $x-y+k$ derived from an abelian group. The construction of the groupoid of Theorem 3.4 will be divided into several lemmas.

We shall be considering two types of sequences of positive or negative integers, $U = \{u_1, u_2, \dots, u_n, \dots\}$. If $u_n = u_{n-1} + u_{n-2}$ for $n = 3, 4, \dots$, U is a Fibonacci sequence or, briefly, F -sequence. As is well known, for large n , $u_{n+1} \sim (1 + \sqrt{5})u_n/2$; thus if $u_1^2 + u_2^2 \neq 0$, then as $n \rightarrow \infty$, $|u_n| \rightarrow \infty$ and u_n remains eventually always positive or always negative. Furthermore, if $u_n = 2u_{n-2} - u_{n-3}$ for $n = 4, 5, \dots$, we call U an A -sequence.

Lemma 3.5 shows that in general two F -sequences are disjoint, i.e., no term of one appears as a term of the other. This fact is used to get similar information about A -sequences in Lemmas 3.7 and 3.8. The construction of the desired groupoid f is carried out in Lemma 3.9.

We will need the notion "for almost all integers." A predicate P about the integers is true for almost all integers if $\lim_{n \rightarrow \infty} P_n/2n = 1$, where P_n is the cardinality of $\{i: -n \leq i \leq n, P \text{ true of } i\}$.

LEMMA 3.5. *If $U = \{u_1, u_2, \dots\}$ is an F -sequence and v_1 is an integer then for almost all v_2 the F -sequence $v_1, v_2, \dots$ has at most the element v_1 in U .*

This lemma is proved for positive sequences in [6]; similar reasoning establishes the lemma in general.

LEMMA 3.6. *If $a_1, a_2, a_3, \dots$ is an A -sequence and $d_n = (-1)^n(a_n - a_{n-1})$ then $d_1, d_2, \dots$ is an F -sequence.*

The proof is left to the reader.

LEMMA 3.7. *If y_1, y_2 are not consecutive terms of the A -sequence $a_1, a_2, a_3, \dots$ then for almost all y_3 the A -sequence $y_1, y_2, y_3, \dots$ has*

no pair of consecutive terms y_m, y_{m+1} coinciding with any pair a_n, a_{n+1} .

PROOF. Consider the F -sequence $-(a_1 - a_2), (a_2 - a_3), \dots, (-1)^n(a_n - a_{n+1}), \dots$, the negative of this sequence, and the F -sequence $Z_1, Z_2, \dots$ beginning with $Z_1 = -(y_1 - y_2)$ and Z_2 so chosen that no Z_n is of the form $(-1)^n(a_n - a_{n+1})$ nor of the form $(-1)^{n+1}(a_n - a_{n+1})$. Define $y_3, y_4, \dots$ so that $y_2 - y_3 = Z_2, -(y_3 - y_4) = Z_3, \dots$. Then $y_1, y_2, y_3, \dots$ is an A -sequence. For no $m > 1$ and n do we have

$$(-1)^m(y_m - y_{m+1}) = (-1)^n(a_n - a_{n+1}),$$

or

$$(-1)^m(y_m - y_{m+1}) = (-1)^{n+1}(a_n - a_{n+1}).$$

In particular we cannot have $y_m - y_{m+1} = a_n - a_{n+1}$ for any m . Hence no pair y_m, y_{m+1} is of the form a_n, a_{n+1} .

From Lemma 3.7 follows

LEMMA 3.8. *If y_1, y_2 are not consecutive terms of the A -sequences $A_1, \dots, A_n$, then for almost all y_3 the A -sequence $y_1, y_2, y_3, \dots$ has no pair of consecutive terms coinciding with any pair of consecutive terms of any of the sequences $A_1, \dots, A_n$.*

Let Z denote the set of integers $\{0, \pm 1, \pm 2, \dots\}$.

LEMMA 3.9. *There is a function $f: Z \times Z \rightarrow Z$ with (1): $f(x, f(y, x)) = 2x - y$ and (2): $f(0, 0) = f(0, -1)$.*

PROOF. If f satisfies (1) and $f(x_1, x_2) = x_3$ it follows that $f(x_2, x_3) = 2x_2 - x_1$. So if $f(x_2, x_3)$ is denoted x_4 we have $x_4 = 2x_2 - x_1$. Generally, if for $n \geq 4$, x_n is defined by $f(x_{n-2}, x_{n-1}) = x_n$ we see that $x_1, x_2, x_3, \dots$ is an A -sequence.

We shall construct f as the union of functions $f_1, f_2, \dots$ defined on disjoint domains. Set $f_1(0, 0) = 1$. If f_1 is to satisfy (1) then $f_1(0, 1) = 0, f_1(1, 0) = 2, \dots$. A simple induction shows that f_1 is the restriction of the function $x - y + 1$ and hence is well defined on its domain.

Observe that $(0, -1)$ is not in the domain of f_1 . Set $f_2(0, -1) = 1$ and then by (1), $f_2(-1, 1) = -2, f_2(1, -2) = 3, \dots$. The domain of f_2 is simply the translate by the vector $(-1, -1)$ of the domain of f_1 less $(0, 0), (0, 1), (1, 0)$. It is then a simple matter to show that the domain of f_2 is disjoint from the domain of f_1 .

Having defined $f_1, \dots, f_k$, we define $f_{k+1}, k \geq 2$, as follows. Let (y_1, y_2) be a point closest to the origin in $Z \times Z - \bigcup_{i=1}^k \text{domain } f_i$. Choose y_3 so the A -sequence $y_1, y_2, y_3, \dots$ has no pair of consecutive terms (y_i, y_{i+1}) in $\bigcup_{i=1}^k \text{domain } f_i$. Then let $f_{k+1}(y_i, y_{i+1}) = y_{i+2}$ for

$i \geq 1$. In this manner an (infinite) sequence of functions $f_1, \dots, f_n, \dots$ is constructed whose domains collectively fill $Z \times Z$. The union of the f_n 's thus defines an $f: Z \times Z \rightarrow Z$ satisfying (1) and (2).

Now it is a brief matter to provide the

PROOF OF THEOREM 3.4. The f of Lemma 3.9 is not a quasigroup since $f(0, 0) = f(0, -1)$. Moreover any f satisfying (1) satisfies $LRLR = I$ since

$$f(x, f(f(x, f(y, x)), x)) = f(x, f(2x - y, x)) = 2x - (2x - y) = y.$$

This ends the proof.

The f of Lemma 3.9 can be used to obtain a stronger result, namely

THEOREM 3.10. *The free groupoid in one letter for the identity $LRLR = I$, $(F_1(LRLR = I))$, is not a quasigroup.*

PROOF. Observe that the subgroupoid of f generated by $\{0\}$ contains 1 and -1 and thus at least two solutions of the equation $f(0, x) = 1$. Thus L_0 is not a bijection. Hence R_0 is not a bijection, in particular, not a surjection. But if $F_1(LRLR = I)$ were a quasigroup then right translation in any one-generated model of $LRLR = I$ would be surjective since any such model is a homomorphic image of $F_1(LRLR = I)$. This contradiction proves the theorem.

BIBLIOGRAPHY

1. Garrett Birkhoff, *On the structure of abstract algebras*, Proc. Cambridge Philos. Soc. **31** (1935), 433-454.
2. J. Kalicki, *The number of equationally complete classes of equations*, Nederl. Akad. Wetensch. Proc. Ser. A **58** (1955), 660-662.
3. D. Scott, *Equationally complete extensions of finite algebras*, Nederl. Akad. Wetensch. Proc. Ser. A **59** (1956), 35-38.
4. R. Artzy, *On loops with a special property*, Proc. Amer. Math. Soc. **6** (1955), 448-453.
5. S. K. Stein, *On the foundations of quasigroups*, Trans. Amer. Math. Soc. **85** (1957), 228-256.
6. ———, *The intersection of Fibonacci sequences*, Michigan Math. J. **9** (1962), 399-402.

UNIVERSITY OF CALIFORNIA, DAVIS