

# FINITE MODELS FOR LAWS IN TWO VARIABLES

A. K. AUSTIN

The object of this paper is to show that any law involving only two variables, at least one of which occurs on both sides of the law, and  $n$ -ary operators,  $n > 0$ , has a finite model. A law [1, p. 439] is an equation in variables and finitary operators, e.g. the associative law. A model is an algebraic system with finitary operators, i.e. a universal algebra [2, p. 94]. By finite model we mean a nontrivial finite model i.e. of order at least two.

§§1 and 2 show how this result is obtained for a single binary operator. In §3 the general result is obtained and also examples are given showing that the result is not true for laws involving nullary operators or more than two variables.

**1. Word polynomials.** In this section  $w$  will be a word in variables and the binary operator  $\rho$ .

The *length* of  $w$  is defined to be the number of occurrences of variables in  $w$ .

The *word polynomial*  $p_w(\lambda, \mu)$  of the word  $w$  is a polynomial in two variables  $\lambda$  and  $\mu$  defined inductively on the length of  $w$  as follows,

if  $w$  is a single variable then  $p_w(\lambda, \mu) \equiv 1$ ,

if  $w \equiv w_1 w_2 \rho$  then  $p_w(\lambda, \mu) \equiv \lambda p_{w_1}(\lambda, \mu) + \mu p_{w_2}(\lambda, \mu)$ .

From this definition the following lemmas can be proved inductively.

**LEMMA 1.** *If  $w$  is a word involving the variable  $x$  only then replacing  $yz\rho$  by  $\lambda y + \mu z$  in  $w$  gives a polynomial in  $\lambda, \mu$  and  $x$  which has the form  $p_w(\lambda, \mu)x$ .*

**LEMMA 2.** *If  $w$  has length at least two then  $p_w(\lambda, \mu) \equiv \lambda^n + \mu^m + \lambda\mu q(\lambda, \mu)$  where  $m$  and  $n$  are positive integers and  $q(\lambda, \mu)$  is a polynomial in  $\lambda$  and  $\mu$ .*

**LEMMA 3.** *If  $\lambda_0$  and  $\mu_0$  are integers such that  $\lambda_0 + \mu_0 = 1$ , then  $p_w(\lambda_0, \mu_0) = 1$ .*

## 2. The result for a binary operator.

**THEOREM 1.** *Let  $w(x, y)$  and  $w'(x, y)$  be two words in variables  $x$  and  $y$*

---

Received by the editors February 3, 1966.

and the binary operator  $\rho$  such that  $x$  occurs in both  $w$  and  $w'$ . Then there exist nonnegative integers  $\lambda_0, \mu_0$  and  $k, k > 1$ , such that if  $S = \{0, 1, 2, \dots, k-1\}$  and the binary operator  $\alpha$  is defined on  $S$  by  $xy\alpha \equiv \lambda_0 x + \mu_0 y \pmod{k}$  then  $(S, \alpha)$  is a finite model for the law  $w(x, y) = w'(x, y)$ .

PROOF. If both  $w$  and  $w'$  have length greater than one then  $w = w'$  is satisfied by  $(S, \alpha)$  where  $S = \{0, 1\}$  and  $\alpha$  is defined on  $S$  by  $xy\alpha = 0$ . In this case  $\lambda_0 = \mu_0 = 0$  and  $k = 2$ . We may assume from henceforth that  $w'(x, y) \equiv x$  and also that  $w(x, y)$  has length at least two.

In  $w(x, y)$  replace  $z\rho$  by  $\lambda z + \mu v$  to give a polynomial in  $\lambda, \mu, x$  and  $y$  of the form  $a(\lambda, \mu)x + b(\lambda, \mu)y$  where  $a(\lambda, \mu) + b(\lambda, \mu) \equiv p_w(\lambda, \mu)$ .

If  $a(\lambda, \mu)$  contains the term of the form  $\lambda^n, n > 0$ , let  $\lambda_0 = 1, \mu_0 = 0$  and  $k = 2$ . Then  $a(\lambda_0, \mu_0) = 1$  and  $b(\lambda_0, \mu_0) = 0$  by Lemma 2. Hence if  $S = \{0, 1\}$  and the binary operator  $\alpha$  is defined on  $S$  by  $xy\alpha = x$  then  $(S, \alpha)$  is a finite model for  $w(x, y) = x$ . We may therefore assume that  $a(\lambda, \mu)$  contains no term  $\lambda^n$  or  $\mu^m$  and therefore (by Lemma 2) that  $b(\lambda, \mu)$  contains the terms of the form  $\lambda^n$  and  $\mu^m, n, m > 0$ .

Since  $x$  occurs in  $w, a(\lambda, \mu) \neq 0$  and so we have that  $a(\lambda, \mu) \equiv \lambda\mu a_1(\lambda, \mu)$  where  $a_1(\lambda, \mu)$  is a polynomial  $\neq 0$ . In  $a(\lambda, \mu)$  replace  $\lambda$  by  $1 - \mu$  to give a polynomial  $c(\mu)$ .  $c(\mu)$  will contain  $\mu$  as factor for let  $d(\lambda)\mu^n, n > 0$ , be the sum of the terms in  $a(\lambda, \mu)$  involving the least power of  $\mu$ . Since  $d(\lambda)$  contains only positive coefficients  $d(1) \neq 0$ . Thus there is a term  $d(1)\mu^n$  in  $c(\mu)$ .

Let  $n$  be the degree of the polynomial  $c(\mu) - 1$  and consider the set  $\{c(t) - 1 \mid 0 \leq t \leq 2n\}$ . There exists at least one integer value of  $t$  for which  $|c(t) - 1| \neq 1$ . Let  $\mu_0$  be the smallest such  $t$  and let  $k = |c(\mu_0) - 1|$  if this is not 0 otherwise  $k = 2$ . Let  $\lambda_0$  be the least nonnegative residue of  $(1 - \mu_0) \pmod{k}$ . Then  $a(\lambda_0, \mu_0) \equiv c(\mu_0) \pmod{k}$ , but  $c(\mu_0) - 1 \equiv 0 \pmod{k}$  and so  $a(\lambda_0, \mu_0) \equiv 1 \pmod{k}$ . Since  $a(\lambda, \mu) + b(\lambda, \mu)$  is a word polynomial and  $\lambda_0 + \mu_0 \equiv 1 \pmod{k}$  we have, by Lemma 3, that  $a(\lambda_0, \mu_0) + b(\lambda_0, \mu_0) \equiv 1 \pmod{k}$ . Hence  $b(\lambda_0, \mu_0) \equiv 0 \pmod{k}$  and so  $a(\lambda_0, \mu_0)x + b(\lambda_0, \mu_0)y \equiv x \pmod{k}$  for  $x$  and  $y$  in  $S = \{0, 1, 2, \dots, k-1\}$ . Thus defining the binary operator  $\alpha$  on  $S$  by  $xy\alpha \equiv \lambda_0 x + \mu_0 y \pmod{k}$   $(S, \alpha)$  is a finite model for the law  $w(x, y) = x$ .

### 3. The result for $n$ -ary operators, $n > 0$ .

THEOREM 2. Let  $w(x, y)$  and  $w'(x, y)$  be words in variables  $x$  and  $y$  and  $h$  operators  $\rho_1, \dots, \rho_h$  where  $\rho_i$  is an  $n_i$ -ary operator,  $n_i > 0$ , such that  $x$  occurs in both  $w$  and  $w'$ . Then there exist nonnegative integers  $\beta(i, j_i), 1 \leq i \leq h, 1 \leq j_i \leq n_i$  and  $k, k > 1$  such that if  $S = \{0, 1, 2, \dots, k-1\}$  and the  $n_i$ -ary operator  $\alpha_i, 1 \leq i \leq h$  is defined on  $S$  by

$$x_1 x_2 \cdots x_{n_i} \alpha_i \equiv \beta(i, 1)x_1 + \beta(i, 2)x_2 + \cdots + \beta(i, n_i)x_{n_i} \pmod{k}$$

then  $(S, \alpha_1, \alpha_2, \dots, \alpha_h)$  is a finite model for the law  $w(x, y) = w'(x, y)$ .

PROOF. We first obtain words  $w_1$  and  $w'_1$  from the words  $w$  and  $w'$  respectively by applying the following operation to the  $\rho_i$  occurring in  $w$  and  $w'$ .

If  $n_i = 1$  omit  $\rho_i$ .

If  $n_i > 1$  replace  $x_1x_2 \dots x_{n_i}\rho_i$  by  $x_1x_2\rho x_3\rho x_4 \rho \dots x_{n_i}\rho$ .

Thus  $w_1$  and  $w'_1$  are words in  $x, y$  and the binary operator  $\rho$  and  $x$  occurs in both  $w_1$  and  $w'_1$ . Hence by Theorem 1 there exist non-negative integers  $\lambda_0, \mu_0$  and  $k, k > 1$ , such that if  $S = \{0, 1, 2, \dots, k-1\}$  and the binary operator  $\alpha$  is defined on  $S$  by  $xy\alpha \equiv \lambda_0x + \mu_0y \pmod{k}$  then  $(S, \alpha)$  is a finite model for the law  $w_1(x, y) = w'_1(x, y)$ .

Define the  $n_i$ -ary operator  $\alpha_i, 1 \leq i \leq h$ , on the set  $S$  as follows.

If  $n_i = 1, x\alpha_i = x$ .

If  $n_i > 1, x_1x_2 \dots x_{n_i}\alpha_i = x_1x_2\alpha x_3\alpha \dots x_{n_i}\alpha$ . It follows from the construction of  $w_1$  and  $w'_1$  from  $w$  and  $w'$  that  $(S, \alpha_1, \dots, \alpha_h)$  is a finite model for  $w(x, y) = w'(x, y)$ . Finally it follows by induction on the order of the operators and taking least nonnegative residues  $\pmod{k}$  that  $\alpha_i$  is defined by  $x_1x_2 \dots x_{n_i}\alpha_i \equiv \beta(i, 1)x_1 + \dots + \beta(i, n_i)x_{n_i} \pmod{k}$  where the  $\beta(i, j_i)$  are nonnegative integers, for  $1 \leq i \leq h, 1 \leq j_i \leq n_i$ .

It can be seen that the result does not hold in the case of nullary operators by considering the law  $yx\rho\alpha\rho = x$ , (1) where  $\rho$  is a binary operator and  $\alpha$  is a nullary operator. By multiplying (1) on the right by  $\alpha$  we have  $yx\rho\alpha\rho\alpha = x\alpha\rho$ , (2) and substituting  $yx\rho$  for  $y$  and  $\alpha$  for  $x$  in (1) gives  $yx\rho\alpha\rho\alpha\rho = \alpha$ , (3). From (2) and (3) we have  $x\alpha\rho = \alpha$  and applying this to (1) gives  $\alpha = x$ . Hence also  $\alpha = y$  and so  $x = y$ . Thus (1) has no nontrivial model. Similarly the law  $yx\rho z\rho = x$  containing three variable  $x, y$  and  $z$ , implies  $x = y$  and hence has no nontrivial model.

#### BIBLIOGRAPHY

1. Garrett Birkhoff, *On the structure of abstract algebras*, Proc. Cambridge Philos. Soc. 31 (1935), 433-454.
2. A. G. Kurosh, *Lectures on general algebra*, Chelsea, New York, 1963.

UNIVERSITY OF SHEFFIELD, ENGLAND