ON COMPARISON OF FINITE ALGEBRAS

J. KALICKI

Introduction. In this paper we shall describe an effective procedure to determine in a finite number of steps whether two abstract algebras A' and A'' of finite order have:

(i) the same set of laws,

(ii) the set of laws of one of them is included in the set of laws of the other,

(iii) distinct sets of laws,

(iv) overlapping sets of laws.

The procedure is a generalization of certain results obtained by the author in case of truth-tables.[1]

Some parts of the paper *On the structure of finite algebras* by G. Birkhoff[2] will be presupposed, namely:

(i) the definition of an abstract algebra $A = (\mathfrak{C}, F)$ and of its order (§2, pp. 433–434),

(ii) the definition of the direct product of abstract algebras (§7, pp. 437–438),

(iii) the definition of an abstract algebra of species Σ_ρ and of a uniform operator (§8),

(iv) the definition of a function ϕ of rank n associated with the species Σ_ρ (§9, Definition 2),

(v) the idea of a substitution ξ of elements of an algebra for each primitive symbol of a function ϕ and of the resulting value $\xi(\phi)$ of the function (§9, p. 439),

(vi) the definition of a law of an algebra (§9, Definition 3),

(vii) the idea of a law of a set of algebras (§9, p. 439),

(viii) the theorem that the set of laws of any aggregate of algebras A_i is the same as that of the direct product A of all the A_i (Corollary 2, p. 440).

The notation used by Birkhoff in the paper referred to will be followed without further explanation.

$L(A_0)$ will stand for the set of laws of any algebra A_0.

1. We first give a test to determine whether $A' = (\mathfrak{C}', F)$ and $A'' = (\mathfrak{C}'', F)$ are such that $L(A') = L(A'')$ or not, where A' and A'' are two abstract algebras of finite orders m' and m'' respectively, and of the same species Σ_ρ.

We form the direct product

$$A = (\mathfrak{C}, F)$$

of A' and A''. A is, of course, of order $m'm'' = m$, and of species Σ_ρ.

The letters A', A'', A, $\mathfrak{C}'$, $\mathfrak{C}''$, $\mathfrak{C}$, F, m', m'', m will have the above meaning throughout the paper.

Now $L(A') = L(A'')$ if and only if every equation $\phi = \phi'$ between two functions ϕ and ϕ' associated with species Σ_ρ has property $P(\mathfrak{C})$, where property $P(\mathfrak{C})$ is defined as follows:

DEFINITION 1. An equation $\phi = \phi'$ between two functions ϕ and ϕ' associated with species Σ_ρ has property $P(\mathfrak{C})$ if and only if one of the following conditions is satisfied:

(i) $\phi = \phi'$ is a law of both A' and A'',

(ii) $\phi = \phi'$ is a law neither of A' nor of A''.

DEFINITION 2. An equation $\phi = \phi'$ between two functions ϕ and ϕ' associated with species Σ_ρ has property $Q(\mathfrak{C})$ (is a $Q(\mathfrak{C})$-equation) if and only if it has not the property $P(\mathfrak{C})$.

Thus $\phi = \phi'$ is a $Q(\mathfrak{C})$-equation if and only if it is a law of A' without being a law of A'' or vice versa, and $L(A') = L(A'')$ if and only if there are no $Q(\mathfrak{C})$-equations.

It is easy to see that the necessary and sufficient condition for $\phi = \phi'$ to be a $Q(\mathfrak{C})$-equation is that the two following conditions are satisfied:

(i') there is a substitution ξ_0 of the elements of $\mathfrak{C}$ for the primitive symbols of ϕ and ϕ' such that $\xi_0(\phi) \neq \xi_0(\phi')$,

(ii') for every substitution ξ of the elements of $\mathfrak{C}$ for the primitive symbols of ϕ and ϕ' if $\xi(\phi) = [x_1, x_2]$ and $\xi(\phi') = [x_1', x_2']$, then $x_1 = x_1'$, or for every substitution ξ of the elements of $\mathfrak{C}$ for the primitive symbols of ϕ and ϕ' if $\xi(\phi) = [x_1, x_2]$ and $\xi(\phi') = [x_1', x_2']$, then $x_2 = x_2'$.

Condition (i') states in fact that $\phi = \phi'$ is not a common law of A' and A'', while condition (ii') states that $\phi = \phi'$ is either a law of A' or of A''.

We shall write $[\phi = \phi']^n$ if the number of *different* primitive symbols in $\phi = \phi'$ equals n.

We prove now:

THEOREM 1. *If $[\phi = \phi']^{n > m}$ is a $Q(\mathfrak{C})$-equation, then there is an equation $[\psi = \psi']^{n \leq m}$ which is a $Q(\mathfrak{C})$-equation.*

PROOF. Suppose that $[\phi = \phi']^{n>m}$ is a $Q(\mathfrak{C})$-equation. Construct an equation $\psi = \psi'$ by identifying in $\phi = \phi'$ any two primitive symbols if and only if the same element of $\mathfrak{C}$ was substituted for them in ξ_0. Since there are only m elements of $\mathfrak{C}$, we obtain $[\psi = \psi']^{n \leq m}$. Moreover $\psi = \psi'$ is a $Q(\mathfrak{C})$-equation.

Let ϕ_t^n stand for any function associated with Σ_ρ such that:

(i) the rank of ϕ_t^n equals t,

(ii) the number of different primitive symbols in ϕ_t^n is n.

Form all the substitutions ξ of the elements of $\mathfrak{C}$ for the primitive symbols of ϕ_t^n. Let the substitutions ξ be effected in a definite fixed order $\xi_1, \xi_2, \cdots, \xi_k$, say, in the lexicographical order.

DEFINITION 3. The finite and ordered sequence of values

$$\xi_1(\phi_t^n), \, \xi_2(\phi_t^n), \, \cdots, \, \xi_k(\phi_t^n)$$

will be called the $\mathfrak{C}$-sequence of ϕ_t^n.

REMARK 1. Clearly $k = m^n$, and hence if $\phi^{n'}$ and $\psi^{n''}$ have the same $\mathfrak{C}$-sequence, then $n' = n''$. It follows that the primitive symbols of the $\phi^{n'}$ and the $\psi^{n''}$ can be made respectively identical by a suitable renaming.

The number of all possible $\mathfrak{C}$-sequences of arbitrary ϕ^n's does not exceed m^{m^n}, and the number of all possible $\mathfrak{C}$-sequences of arbitrary $\phi^{n \leq m}$ does not exceed

$$\sum_{i=1}^{m} m^{m^i} = n_0.$$

Since there exist functions of any rank $t = 1, 2, \cdots$, there is an integer

$$t_0 \leq n_0 + 1$$

such that there are no functions $\phi_{t_0}^{n \leq m}$ with the $\mathfrak{C}$-sequences different from the $\mathfrak{C}$-sequences of all the functions $\phi_{t < t_0}^{n \leq m}$.

We prove now:

THEOREM 2. *For every function* $\phi^* = \phi_{t \geq t_0}^{n \leq m}$, *there is a function* $\psi_{t < t_0}^{n \leq m} = \psi^*$ *such that* ϕ^* *and* ψ^* *have the same* $\mathfrak{C}$-*sequence, and the same primitive symbols.*

PROOF. For $t = t_0$, the theorem follows directly from the definition of t_0 in virtue of Remark 1.

Consider $\phi^* = \phi_{t_0+1}^{n \leq m}$. By the definition of rank,

$$\phi^* = f_i(\phi_{t_1 \leq t_0}^{n_1 \leq m}, \, \phi_{t_2 \leq t_0}^{n_2 \leq m}, \, \cdots, \, \phi_{t_{k_i} \leq t_0}^{n_{k_i} \leq m}),$$

where $\max_{j=1, \ldots, k_i} t_j = t_0$. Hence, by definition of t_0, there are functions $\psi_{t'_j < t_0}^{n_j \leq m}$ such that the $\mathfrak{C}$-sequences of $\psi_{t'_j}^{n_j}$ are the same as the $\mathfrak{C}$-sequences of $\phi_{t_j}^{n_j}$ for $j = 1, 2, \cdots, k_i$. Moreover, the primitive symbols of $\psi_{t'_j < t_0}^{n_j \leq n}$ and $\phi_{t_j \leq t_0}^{n_j \leq m}$ are the same in number, and hence may be considered as respectively identical (cf. Remark 1).

Let

$$\psi^* = f_i(\psi_{t'_1 < t_0}^{n_1 \leq m}, \psi_{t'_2 < t_0}^{n_2 \leq m}, \cdots, \psi_{t'_{k_i} < t_0}^{n_{k_i} \leq m}).$$

Clearly ψ^* and ϕ^* have the same $\mathfrak{C}$-sequence. Moreover, the rank of $\psi^* = \max_{j=1, \ldots, k_i} t'_j + 1 \leq t_0$, and the primitive symbols of ψ^* are the same as the primitive symbols of ϕ^*. This completes the proof of Theorem 2, for $\phi_{t_0+1}^{n \leq m}$. The extension to an arbitrary $\phi_{t=t_0+k}^{n \leq m}$ follows by induction on k.

Let now $\mathcal{J}$ stand for the family of equations $[\psi = \psi']^{n \leq m}$ such that $\psi = \psi_{t < t_0}$ and $\psi' = \psi'_{t < t_0}$.

Theorem 3. *If $\phi = \phi'$ is a $Q(\mathfrak{C})$-equation not in $\mathcal{J}$, then there is in $\mathcal{J}$ a $Q(\mathfrak{C})$-equation $\psi = \psi'$.*

Proof. Let $\phi = \phi'$ be a $Q(\mathfrak{C})$-equation not in $\mathcal{J}$. If $[\phi = \phi']^{n > m}$, then by Theorem 1 there is a $Q(\mathfrak{C})$-equation $[\chi = \chi']^{n \leq m}$. Hence both functions χ and χ' are such that $\chi = \chi^{n \leq m}$ and $\chi' = \chi'^{n \leq m}$. If $\chi = \chi_{t \geq t_0}^{n \leq m}$, then, by Theorem 2, there is a function $\psi_{t < t_0}^{n \leq m}$ such that χ and ψ have the same $\mathfrak{C}$-sequence and the same primitive symbols. Similarly, if $\chi' = \chi'^{n \leq m}_{t \geq t_0}$, there is a function $\psi'^{n \leq m}_{t < t_0}$ such that the $\mathfrak{C}$-sequences and the primitive symbols of χ' and ψ' respectively coincide. Hence if $\chi = \chi'$ is a $Q(\mathfrak{C})$-equation, $\psi = \psi'$ is also a $Q(\mathfrak{C})$-equation. Moreover, $\psi = \psi'$ is in $\mathcal{J}$ and this completes the proof of Theorem 3.

The contraposition of Theorem 3 renders:

Theorem 4. *If no equation of $\mathcal{J}$ is a $Q(\mathfrak{C})$-equation, then there are no $Q(\mathfrak{C})$-equations, and hence all the equations have property $P(\mathfrak{C})$.*

Theorem 4 gives us an effective procedure to find whether $L(A') = L(A'')$ or not. Namely, we construct the family $\mathcal{J}$ and check whether there is a $Q(\mathfrak{C})$-equation in $\mathcal{J}$ or not.

In the first case $L(A') \neq L(A'')$, in the second case $L(A') = L(A'')$. The checking is always possible since the number of the elements of $\mathcal{J}$ is finite provided we do not count more than once equations which differ only in the notation used for the primitive symbols.

2. In case $L(A') \neq L(A'')$ it may happen that $L(A') \subset L(A'')$ or vice versa.

To decide whether this is the case it is sufficient to consider the

direct product A of A' and A''. If $L(A)=L(A')$, we obtain that $L(A')\subset L(A'')$, if $L(A)=L(A'')$, we obtain that $L(A'')\subset L(A')$, if neither $L(A)=L(A')$ nor $L(A)=L(A'')$, we conclude that $L(A')$ and $L(A'')$ overlap. This is so since for no A' and A'', $L(A')$ and $L(A'')$ can be disjoint, since $a=a$ is a law of every two algebras $(\mathbb{C}', F)$ and $(\mathbb{C}'', F)$.

3. No difficulty is encountered if we wish to extend the results to algebras of finite orders, the operators of which are not uniform, nor in the case of algebras which are not of the same species.

In the latter case the sets of laws of the respective algebras cannot be identical. This is clear if we note that if f is an operator of A' $=(\mathbb{C}', F')$ but not of $A''=(\mathbb{C}'', F'')$, then $f(a, \cdots, b)=f(a, \cdots, b)$ is a law of A' without being a law of A''. Also $a=a$ is a law of both A' and A''. Hence the only case of interest is when $L(A'')\subset L(A')$. This may occur if $F''\subset F'$. If $F''\subset F'$ we consider the algebras A'' $=(\mathbb{C}'', F'')$ and $A'''=(\mathbb{C}', F'')$. Clearly, $L(A''')\subset L(A')$, and hence if $L(A'')\subset L(A''')$, then $L(A'')\subset L(A')$, and A'' and A''' are already of the same species.

There is, however, an essential difficulty in extending the above results to algebras of infinite order, and this last problem remains open.

UNIVERSITY OF LEEDS AND
    UNIVERSITY OF CALIFORNIA