An Analysis of Logical Substitution.

By H. B. Curry.

Contents. *

Originally published in the American Journal of Mathematics, Vol. 51, No. 3 (July 1929), pg. 363-384 by Haskell Brooks Curry. According to U.S. laws, the original work is public domain as of Jan 1, 2025. This document is a digital recreation in LaTeX, source repo is at github.com/jonathan-mfung/AnAnalysisofLogicalSubstitution_Curry1929. Typeset by Jonathan Fung, contact at `jonathanfung2000@gmail.com`. *The work was recreated as faithfully as possible, but is not pixel-perfect.*

I.

Mathematical Logic has been defined as an application of the formal methods of mathematics to the domain of Logic.† Logic, on the other hand, is the analysis and criticism of thought.‡ In accordance with these definitions, the essential purpose of mathematical logic is the construction of an abstract (or strictly formalized) theory, such that when its fundamental notions are properly interpreted, there ensues an analysis of those universal principles in accordance with which valid thinking goes on. The term analysis here means that a certain rather complicated body of knowledge is exhibited as deriveable from a much simpler body assumed at the beginning. Evidently the simpler this initial knowledge, and the more explicitly and carefully it is set forth, the more profound and satisfactory is the analysis concerned.

In the present paper I propose to take some preliminary steps toward a theory of logic in which the assumed initial knowledge is simpler than in any existing theory with which I am acquainted. Before this is done, however, it is necessary to consider somewhat in detail what is meant by the phrase "abstract theory," and what is the significance of such a theory for the analysis of thought.

* The three parts of this paper are to a certain extent independent of one another. However, certain definitions needed in Part III are given in the last six paragraphs of Part II.

† Hilbert, D., and Ackermann, W., *Grundzüge der theoretischen Logik*, 1928, p. 1.

‡ Johnson, W. E., *Logic*, Part I, Cambridge (1921), p. xiii.

The object of this discussion is to see just how the assumed knowledge enters into the theory; for this purpose we shall need to be explicit, even at the risk of repeating what has already been better said by others.

Certain ideas concerning the nature of an abstract theory can be disposed of at once. In the first place the naive notion that such a theory consists of a set of primitive ideas and propositions together with their consequences by the laws of pure logic, must be dismissed on the ground of its circularity. Again it is said that an abstract theory is one from which all meaning has been abstracted. This requires that the sense of the term meaning be explained. If we take the term meaning, as applied to objects, to signify the totality of properties (of those objects) which are directly apprehensible to our intuition, then every object presented to the mind has meaning, and a meaningless theory is a contradiction in terms. Even a symbol cannot be meaningless in this sense; for either it denotes some object, or else it is itself the object, and so has meaning. If we use the word meaning in some other sense, then it loses its significance as related to the assumed initial knowledge of our theory. Consequently the idea of a meaningless theory must be subjected to further scrutiny.

Let us use the word meaning, as applied to concepts, in the sense of the preceding paragraph. Then, relative to a given theory, we may distinguish two kinds of meanings, which we shall call natural and conventional meanings respectively. Natural meanings are those which are comprehensible a priori in terms of our previous knowledge; conventional meanings those based on relations to the theory itself. Natural meanings we may further subdivide into essential and accidental: essential meanings are those on which the deduction of the theory depends; accidental meanings those which are nonessential. The distinction between these three kinds of meaning is important in what follows.

The distinction between natural and conventional meanings has a counterpart in that between statements of fact and statements of convention. By a statement of fact I mean something of which truth or falsehood can significantly be predicated; by a statement of convention a declaration of intention, definition, or the like. The former corresponds to an act of judgment,the latter to one of volition. Common sense and grammar have long recognized both of these types; yet logicians seem to belittle the latter in that they define the proposition so as to exclude it.* Both these kinds of statement, however, are equally intelligible to a rational mind; in this sense it is false to say that one of them is less significant than the other. As examples of statements of convention we have of

* See Johnson, W. E., *1. c.*, p. 1. Johnson's definition of the proposition is what I have given as the definition of a statement of fact.

course the definitions of technical terms; but not all statements of convention are verbal—for instance the rules of chess, which, by a sufficient amount of circumlocution, may be stated without defining any new terms whatever. The postulates of any branch of mathematics are of this character.

Let us now return to the abstract theory. I suggest that such a theory is characterized by the following: 1) the explicit indication of all essential meanings; 2) the absence, or at least omission from consideration, of accidental meanings; 3) the circumstance that the statements with which the theory begins are conventional, and are, furthermore, sufficiently detailed so that all the acts necessary to the deduction are specified.

To be yet more precise,an abstract theory begins with a set of primitive notions, which, taken collectively, we shall call the *primitive frame*, as follows:

I. Non-Formal Primitive Ideas.*

A set of ideas to each of which a certain amount of essential meaning is attached, although they need not coincide with any ideas previously entertained.† For example:

1. Entities. In order for an object to be considered in the theory at all, it must have some property; this fact we may express by saying it is an entity of one sort or another. These properties must then be among the primitive ideas of the theory; and they must have essential meaning in that they are predicates. In the simplified theory only one such notion is necessary; but in the more complicated ones there are several; e. g. in the Principia Mathematica there are individual, proposition, function, etc., the latter two of various orders and types.

2. Modes of Combination. I.e. processes by means of which entities may be combined to get new entities. These have essential meaning in that they are combinations. It must be specified by rules that the results of combination are entities. In the simple cases only one such notion is necessary, and that a dyadic one; in the more complicated cases the various processes of substitution are of this nature.

3. Assertions. An assertion is a kind of entity, which is of special importance because the object of deduction is to derive new assertions. The idea of assertion has essential meaning only in that it is a predicate applicable to certain entities.

*The term idea is used here to denote an object, not a process of thought.

† *I. e.*, their meaning may be partly conventional.

Ordinarily an assertion is interpreted as a statement to which belief attaches, but this meaning is accidental.

II. FORMAL PRIMITIVE IDEAS.

Ideas which have no essential meanings (except that they are concepts). They must of course be entities and their relations to other parts of the primitive frame will give them conventional meanings.

III. POSTULATES.

All propositions of the theory are statements that certain particular entities are assertions; the postulates are the propositions, if any, which are assumed at the beginning. They are purely conventional.

IV. RULES.

Statements of the processes by means of which new entities* or new propositions maybe constructed. Such statements are of course conventional; moreover they are universal statements (involving the notion of "every" or its equivalent†). They thus differ from propositions not only in that they involve intuitive ideas from which the propositions are free, but also in that they form the methods of transition, rather than the stopping places in the theory. A typical example is the "rule of inference" which may be stated thus: whenever p and $p \supseteq q$ are assertions, then q shall also be an assertion

In addition to the above notions there are yet to be considered those associated with the use of symbolism. Whether these are to be regarded as a part of the theory or as something superposed upon it, is a question which I prefer to leave to the reader to adopt such views as seem best to him. However he may decide, certainly language is necessary in order that the theory may be communicated. The use of this language may involve intuitive operations other than those we have mentioned; it is desirable that these, too, be specified by

* Strictly speaking we should consider in the theory not only statements that an entity is an assertion, but also statements that such and such combinations are entities. But the latter are, in simple cases at least, of so trivial a nature that it is not necessary to give them special prominence.

† Otherwise the rule would make possible the addition of only a finite number of constituents, and these could just as well be added explicitly to the preceding categories of the primitive frame

rules; because otherwise it is not certain that intuitive, knowledge, other than that expressly mentioned, does not creep into the theory. We shall call such rules *symbolic conventions*.

So much for the primitive frame. The abstract theory itself may now be defined as the doctrine built upon such a primitive frame by means of the following processes: 1) the derivation of new propositions, each of which is of the form that such and such an entity is an assertion, by means of the rules; 2) the addition of new ideas by definitions. The latter process may be regarded either as a symbolic matter, governed by symbolic conventions, or as the introduction of a new idea along with postulates and rules to the effect that it is identical with some already existing entity. It is worth emphasizing that since statements that entities are not assertions do not occur among the propositions, such a theory can never lead to a contradiction there.

The importance of such a theory for the analysis of thought lies in the definiteness with which the intuitive knowledge entering into it is set forth. Indeed, so far as the abstract theory itself is concerned, the only knowledge assumed is the appreciation of the essential meanings and conventional statements appearing in the primitive frame. When the theory is interpreted the additional knowledge that must be brought to bear consists of the following: that the concepts which we substitute for the primitive ideas have the necessary essential meanings, and that the conventional statements in the primitive frame correspond to facts. In both cases the required information is precisely specified.

On the philosophic nature of such a theory, its relations to the symbolism used in its expression, and to the various concrete theories obtained by interpreting it, it suffices to say that such questions are largely metaphysical, and therefore irrelevant to the present discussion. It is by no means self-evident that the best interests of science are served by adopting any one theory to the exclusion of all others; any more than it is desirable that two persons following the same argument should have the same mental imagery.*

The next point to which I wish to direct the reader's attention is the cardinal importance of the rules in any abstract theory related to logic. For the amount of initial knowledge which enters into the first three categories of the primitive frame is slight. In the rules, however, such knowledge is involved in every step of the construction; for we have to pass judgment as to whether the contemplated act is or is not according to Hoyle. These judgments, moreover,

---

* In writing the foregoing account I have naturally made use of any ideas I may have gleaned from reading the literature. The writings of Hilbert are fundamental in this connection. I hope that I have added clearness to certain points where the existing treatments are obscure.

are the only ones which are required. The rules, therefore, form the port of entry of intelligence; and since nothing can be done without them they represent the atoms of thought, so to speak, into which the reasoning can be decomposed. It follows that in constructing such a theory it is not sufficient merely to reduce the postulates and primitive ideas to their lowest terms; it is even more important to so chose the rules that they involve,in their application, only the simplest actions of the human mind.

Now although the rule of inference, stated above, is simple enough, yet in all current mathematical logics there exist rules which are highly complex. The presence of these complex rules raises the question whether it is possible to formulate a theory which is—1) adequate for the whole of logic, 2) based on a finite number of primitive ideas, postulates, and rules, the last of the same order of complexity as the rule of inference. I believe that it is; indeed steps in that direction have already been taken.* As a preliminary to treating this general problem, I shall discuss in the rest of this paper a special one connected with it; viz., the analysis of the process of substitution. The latter process is one of those complicated rules which occur in practically every logical theory to-day.

The reader will observe that in the theory which results from the analysis the formulas are more complicated, and the deductions required to produce them more lengthy, than would be the case in the older theory. This is inevitable. Indeed if we are to dissect the reasoning into microscopic pieces it is but natural that more of them should be necessary to bring about a given result. Consequently we must adopt a point of view suggested by Hilbert. With each theory there is associated a metatheory in which we reason intuitively about the theory. In this metatheory we can derive more and more complicated rules by showing, in general terms, how any particular consequence of the derived rules can actually be deduced from the primitive ones. The aim of mathematical logic is, in fact, not to reduce mathematics to a formalism, à la *Principia*, in which all steps explicitly appear; but rather to analyze logic with a view to obtaining a greater command over its use, and a more profound understanding of its nature. In this paper we shall adopt this metatheoretic point of view.

II.

The process of substitution referred to above is the insertion of a constant entity for one or more of the variables in a propositional function. The complexity of this process is manifest. For not only is a function of n variables a

* See the paper of Schönfinkel cited below.

distinct concept for every value of n, but the constant may be inserted in any one of the n places, and each such insertion is a distinct act; furthermore, in connection with the universal and existential prefixes,we have a process which virtually amounts to the simultaneous substitution of an entity in two or more distinct places, as a procedure distinct from any of the foregoing. The process of substitution is therefore compound in that it is not one maneuver, but many. Moreover, when these acts of substitution are performed in succession, there are many equivalences between the different possibilities. To take the simplest example: suppose in a given function $\phi(x, y)$ we substitute a for x, and in the result, which is $\phi(a, y)$, we substitute b for y, we have the proposition $\phi(a, b)$; on the other hand, if we first substitute b for y and then a for x, we obtain the very same proposition. Yet these two processes are in no sense identical. The substitution process is therefore not only compound but complex, in the sense that it has structure. Thus there is a considerable amount of information presupposed by the process; and the rules involving it cannot have the maximum possible simplicity.

A notion closely related to substitution is that of transformation of functions. Suppose we regard a function as having inherent in its definition a certain order of its variables. Then permuting these variables in any way, or making two or more of them alike, will produce new functions related to the old; let us call them transforms of the original function, and the operations by which they are produced transformations. If we number the variables consecutively $1, 2, 3, \cdots$, then the transforms for a function of two variables will be—

$$\phi(1, 2),\ \phi(2, 1),\ \phi(1, 1).$$

For three variables there will be 13 transforms, for four variables 75, for five variables 541, etc. It is clear that the process of substituting a series of constants in an arbitrary manner (such that the total number of entities counting repetitions is n) into the original function is equivalent to the substitution of the same entities in a prescribed manner (viz., the first entity into the place of the first variable, the second into that of the second, etc.) into one of the transforms. The study of substitution is thus to a certain degree equivalent to the study of these transformations.

An important step toward the analysis of this situation was made by M. Schönfinkel.* Starting, apparently, from the fact that every logical formula is a combination of constants—the variables being only apparent—he shows

* "Ueber die Bausteine der mathematischen Logik," *Mathematische Annalen*, Vol. 92 (1924), pp. 305-316.

that neither the notions of propositional function (of various orders) nor that of substitution need be assumed as primitive; his formulation of logic is such that variables, real or apparent, do not appear explicitly. His primitive frame is essentially as follows:*

I. NON-FORMAL PRIMITIVE IDEAS.

1. Entity—not mentioned by Schönfinkel, but to be understood essentially as a single notion of the sort mentioned in the general description of an abstract theory above.

2. Application—a mode of combination, the only one in the theory. Two entities x and y combine to give a third entity called the application of x to y and denoted by (xy). The *interpretation* of this is as follows: if x is a function, then (xy) is the result of substituting y for the first variable in x; thus if f denote a function of one variable, (fx) denotes what is ordinarily written $f(x)$, if f is a function of two variables, $((fx)y)$ denotes what is ordinarily written $f(x, y)$, etc. Nothing is said concerning the interpretation of (xy) when x is not a function; if the reader is disturbed over this lack, he may invent one arbitrarily, *e. g.* (xy) may then be equal to x.

3. Assertion. To be understood as in the general description of an abstract theory. Not denoted by any particular symbol; but when a symbol of the form $(((=)x)y)$ (or $x = y$) where x and y may be quite complicated, stands out by itself like an equation in algebra, then the proposition that the corresponding entity is an assertion is to be understood.

II. FORMAL PRIMITIVE IDEAS.

Three, denoted by $(=)$, S and K. In the interpretation $(=)$ is to correspond with identity; S and K are operations in the sense defined by the rules.

Symbolic Conventions.

1. If x and y are any entities whatever, then instead of $(((=)x)y)$ we may write $(x = y)$.

2. If $x_1, x_2, \cdots, x_n$ are any entities, then instead of

$$((\cdots(((x_1x_2)x_3)x_4)\cdots)x_n)$$

* In this presentation I have changed Schönfinkel's formulation in some matters of detail.

we may write $(x_1 x_2 x_3 \cdots, x_n)$.

3. The outside parentheses may be left off in the case of a symbol standing by itself or on either side of the sign $=$.

III. POSTULATES.

None.

IV. RULES.

0. If x and y are entities, then (xy) shall be an entity.

1. $(=)$ shall have the properties of identity. These properties may be specified by a few simple rules; but in this treatment we shall not go into that detail. We shall treat $(=)$ as if it were precisely the intuitive relation of equality.

2. If x and y are any entities, then

$$Kxy = x$$

3. If x, y, z are entities, then

$$Sxyz = xz(yz)$$

4. If X and Y are combinations of S and K, and if there exists an integer n such that by application of the preceding rules we can formally reduce the expressions $Xx_1x_2 \cdots x_n$ and $Yx_1x_2 \cdots x_n$ to combinations of $x_1x_2 \cdots x_n$ which have the same structure, then $X = Y$.

If the above primitive frame were a part of a general theory of logic, the term entity would include not only the various combinations of S and K, but all the notions of logic as well. In the sequel we shall accordingly speak of the application of combinations S and K to various logical notions, and of the resulting notions to each other, just as if these notions had been adjoined to the above frame.

The *raison d'être* of the theory based on this frame is the following fact: Let $x_1, x_2, \cdots, x_n$ be any n entities, and X any combination of them constructed by means of application. Then there exists a unique Y, which is a combination of S and K and independent of $x_1, x_2, \cdots, x_n$ such that

$$X = Yx_1x_2 \cdots x_n.$$

When we recall the interpretation to be given to application we have the following result: given any logical formula built up from functions $f_1, f_2, \cdots, f_m$ and variables $x_1, x_2, \cdots, x_n$ by substitution and rearrangement in any manner; then the formula is expressible in the form

$$Fx_1x_2 \cdots x_m$$

where

$$F = Yf_1f_2 \cdots f_m.$$

Now as already remarked, in the formulas expressing propositions of logic, the variables are only apparent; which means that they are only a device by means of which rather complicated relations among the logical constants may be expressed; these relations, as the preceding argument shows, may also be expressed by means of the operators Y, so that when the Schönfinkel theory is used it is not necessary that variables should appear at all.

The theory of transformation of functions is included in the above as a special case; viz., when there is a single function f and F is a transform.

The theory is, however, open to objection from our point of view because of the complexity of Rule 4. This rule is not mentioned by Schönfinkel; but it is necessary in order that the Y mentioned be unique. In fact, the combinations SK and $K(SKK)$ determine the same X; yet it is evidently not possible to establish their identity by means of the first four rules.

This situation suggests a problem; viz., to find a set of postulates which, when adjoined to the Schönfinkel frame, enable us to dispense with Rule 4. In what follows we shall obtain the solution of a special case under this problem; specifically, we shall find a set of postulates such that, within a certain subclass of combinations of S and K, all the Y's which correspond to the same X may be proved equal by means of these postulates and Rules 0-3. The subclass is one which has particular reference to logical substitution.

To begin with, we make the following definitions (the first three were made by Schönfinkel):*

* We use B and C respectively in place of Schönfinkel's Z and T. Nothing corresponding to W or $C_2, C_3, \cdots$ is defined by him.

$$\begin{aligned}
I &= SKK \\
B &= S(KS)K \\
C_1 &= S(BBS)(KK) \\
C_2 &= BC_1; C_3 = BC_2; \cdots \text{etc.} \\
W &= SS(SK)
\end{aligned}$$

then the reader may verify that whenever $x_0, x_1, x_2 \cdots$ are entities

$$\begin{aligned}
Ix_0 &= x_0 \\
Bx_0x_1x_2 &= x_0(x_1x_2) \\
C_1x_0x_1x_2 &= x_0x_2x_1 \\
C_2x_0x_1x_2x_3 &= x_0x_1x_3x_2 \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
Wx_0x_1 &= x_0x_1x_1
\end{aligned}$$

Also we define multiplication, thus

$$X \cdot Y = BXY$$

This multiplication is associative, and furthermore with respect to it, I is an identical element These properties follow from Rule 4; they may also be proved from the postulates:

$$\begin{aligned}
&C_1(BB(BBB))B = BBBBB \\
&BI = I \\
&C_1BI = I.
\end{aligned}$$

The subclass in question shall now consist of all the combinations formed by multiplication from the C's, W, and I.

Before discussing the significance of this subclass, we turn aside to make some conventions in regard to transformations. Let us redefine a transformation as an operation converting the sequence $1, 2, 3, \cdots$ into the sequence $a_1, a_2, a_3, \cdots$ The latter sequence will, in the cases we consider, have the property that there exists and index m such that: 1) for $i \leqq m$ the a_i are a permutation, with repetitions allowed, but not omissions, of the integers from 1 to $m - p$, $p \geqq 0$, inclusive, 2) for $i > m, a_i = i - p$. Let m be the least integer having this property; then we shall call m the order of the transformation. We shall denote a transformation by writing in brackets the sequence into which it transforms the sequence $1, 2, 3, \cdots$; furthermore, there is no ambiguity if we indicate only the first n terms of the former sequence, if $m \leqq n$.

We shall further agree that a transformation of order m may operate on a function of any number of variables $\geqq m$; and that the effect of the transformation on the function $\phi(1, 2, \cdots, n)$, where $n \geqq m$, shall be the transform $\phi(a_1, a_2, \cdots a_n)$. We shall regard as undefined the effect of a transformation on a function of multiplicity less than the order of the transformation. Then there is one and only one transformation which carries a given function into a given transform.

Multiplication of transformations we now define as follows:

$$[a_1, a_2, a_3 \cdots] \cdot [b_1, b_2, b_3 \cdots] = [a_{b_1}, a_{b_2}, a_{b_3} \cdots] \tag{1}$$

(The product transformation has a finite order, provided that the factors do.)

Suppose, now, that we have a combination, X, of S and K, having the property that there exists a transformation $\alpha = [a_1, a_2 \cdots a_m]$ such that for arbitrary $x_0, x_1, x_2, \cdots x_{m-p}$

$$Xx_0x_1x_2 \cdots x_{m-p} = x_0x_{a_1}x_{a_2} \cdots x_{a_m}$$

where m and p are defined as above. Then we shall say that X corresponds to α. It follows from Rules 0-3 that if X and Y are entities which correspond to transformations α and β, respectively, then $X \cdot Y$ corresponds to $\alpha\beta$.

I now assert that every entity of our subclass corresponds to a transformation; and conversely that every X corresponding to a transformation, is an entity of the subclass. For since the generating entities, the C's, W, and I, correspond to transformations, the first part of the statement follows from the closing sentence of the last paragraph. The last part follows similarly from the fact that every transformation can be obtained by multiplication from permutations of adjacent integers and the transformation $[1, 1.]$ Of course the one-to-oneness of the correspondence depends essentially on Rule 4.

The problem now is to find a set of postulates for the C's and W, from which we may conclude, without the use of Rule 4, that the correspondence between our subclass and the set of all transformations is a simple isomorphism. To this we now turn.

III.

Theorem

1) Let $\mathfrak{A}$ be a system of operators, in which there exists an associative multiplication and an identical element, I.

2) Let this system be generated by operators $W, C_1, C_2, \cdots$ Subject to the postulates

I.	$C_i \cdot C_i = I$	$i = 1, 2, 3, \cdots$	
II.	$C_i \cdot C_{i+1} \cdot C_i = C_{i+1} \cdot C_i \cdot C_{i+1}$	$i = 1, 2, 3, \cdots$	
III.	$C_i \cdot C_j = C_j \cdot C_i$	$i = 1, 2, 3, \cdots$	$j > i + 1$
IV.	$C_i \cdot W = W \cdot C_{i+1}$	$i = 2, 3, 4, \cdots$	
V.	$W \cdot C_1 = W$		
VI.	$W \cdot W \cdot C_2 = W \cdot W *$		
VII.	$W \cdot D_j \cdot W = D_{j-1} \cdot W \cdot D_3 \cdot W \cdot C_2 \cdot C_3 \cdot C_1 \cdot C_2 *$		$j = 3, 4, 5 \cdots$

where

$$D_1 = I$$
$$D_{j+1} = C_j \cdot D_j = C_j \cdot C_{j-1} \cdot C_{j-2} \cdot \cdots \cdot C_1$$

3) Let a correspondence be set up between the system $\mathfrak{A}$ and the system of transformations of finite order as follows:

$$\begin{aligned} W &\sim [1, 1] \\ C_1 &\sim [2, 1] \\ C_2 &\sim [1, 3, 2] \\ C_i &\sim [1, 2, 3, \cdots i - 1, i + 1, i] \end{aligned} \tag{2}$$

and if $A \sim \alpha$, $B \sim \beta$† then $A \cdot B \sim \alpha \cdot \beta$ is defined by (1).
Then, the correspondence so defined is a one-to-one isomorphism.

Proof.

There are four things to prove:

∗VI and VII are equivalent respectively to (6) and (7) (see below). The latter may if desired replace VI and VII.

† Throughout this discussion we use Roman capitals to denote operators of $\mathfrak{A}$, Greek l. c. letters to denote transformations.

1) That to every product expression in $\mathfrak{A}$ there corresponds a unique transformation.

2) That this correspondence is an isomorphism.

3) That if two transformations correspond to two expressions in $\mathfrak{A}$ which are equal by Virtue of I-VII (inclusive), then these transformations are equal.

4) That conversely there corresponds an operator of $\mathfrak{A}$ to each transformation, and any two operators corresponding to the same transformation may be proved equal by I-VII.

Of these four things the first three follow immediately: the first two by definitions; the third because propositions analogous to I-VII are true for transformations.*

It remains, therefore, only to prove the fourth.

By a theorem due to E. H. Moore† postulates I-III insure that the subset of $\mathfrak{A}$ which is obtained from the first $n-1$ C's only is isomorphic with the symmetric group on n letters; the correspondence is established in the same way as here. It follows readily that the subset generated by all the C's is isomorphic with the totality if all those transformations which do not allow repetition. In fact, suppose two such operators of $\mathfrak{A}$ correspond to the same transformation; let n be the largest index appertaining to a C in either one; then the two operators correspond to the same permutation on $n+1$ letters, and therefore, by Moore's result, are equal in virtue of I-III. In the following we shall assume this result as known; and therefore shall often designate operators composed of C's only by means of the transformations corresponding to them.

In order to prove the fourth statement above when W is considered, we shall show that every operator in $\mathfrak{A}$ can be expressed in a certain normal form, and then that one and only one such expression in normal form corresponds to a given transformation.

---

* The only question here is about VII. It follows, however, by definition, that

$$D_i \sim [i, 1, 2, 3, \cdots, i-1]$$

and therefore the proposition analogous to VII is the identity

$$\begin{aligned}&[1,1]\cdot[j, 1{,}2, \cdots, j-1]\cdot[1,1]\\ &\qquad = [j-1, 1, 2, \cdots, j-2]\cdot[1.1]\cdot[3,1,2]\cdot[1,1]\cdot[3,4,1,2].\end{aligned}$$

Both sides here are equal to $[j-1, j-1, 1, 1, 2, 3, \cdots, j-2]$.

† *Proceedings of the London Mathematical Society*, Vol. 28 (1897), p. 357-366. Moore's proof involves some rather complicated theorems in group theory. It is, however, possible to prove the theorem by directly establishing the correspondence.

To obtain such a normal form we introduce the following definitions:

$$\begin{aligned} W_1 &= W \\ W_2 &= C_1 \cdot W_1 \cdot C_2 \cdot C_1 \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ W_{k+1} &= C_k \cdot W_k \cdot C_{k+1} \cdot C_k \end{aligned}$$

it then follows by induction* that

$$\begin{aligned} W_k &= D_k \cdot W \cdot C_2 \cdot C_3 \cdot C_4 \cdots C_k \cdot C_1 \cdot C_2 \cdot C_3 \cdots C_{k-1} \\ &= [k, 1, 2, \cdots k-1] \cdot W \cdot [3, 4, \cdots k+1, 1, 2] \end{aligned}$$

whence,

$$\begin{aligned} W_2 &\sim [1, 2, 2] \\ W_3 &\sim [1, 2, 3, 3] \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ W_k &\sim [1, 2, 3, \cdots k-1, k, k] \end{aligned}$$

The result we wish to prove now follows from a series of lemmas.

Lemma 1. *Every product expression in* $\mathfrak{A}$ *can be reduced to the form*

$$W_{k_q} \cdot W_{k_{q-1}} \cdots W_{k_2} \cdot W_{k_1} \cdot B. \tag{3}$$

where B involves the C's only.

Proof.

First we show that any expression of the form $A \cdot W$ can be reduced to the form $W_k \cdot B$, where A and B involve the C's only. If A is the identical element we are through. If not, consider the C nearest the W; if this is any other than C_1 it can be passed across the W by IV, otherwise we have an expression of the form $A' \cdot C \cdot W$, where A' involves one less C than A.

Now suppose w have reduced $A \cdot W$ to the form $A' \cdot D_j \cdot W \cdot B'$ where A' and B' involve the C's only and A' is not I. Let C_i be that C in A' which is nearest D_j. Four cases can rise: 1) if $i < j-1$, $C_i \cdot D_j = D_j \cdot C_{i+1}$ and since $i+1 > 1$, C_{i+1} can be passed across the W by IV; 2) if $i = j-1$, $C_i \cdot D_j = D_{j-1}$; 3) if $i = j$, $C_i \cdot D_j = D_{j+1}$; 4) if $i > j$, $C_i \cdot D_j = D_j \cdot C_i$, and since $i > j \geqq 1$, C_i can be passed across the W by IV. In all four cases we have reduced the

* This and other proofs by mathematical deduction are such that by repeating the argument a sufficient number of times the formula may be established in any particular case with the use of I-VII.

expression to another one of the same form where the new A' involves one less C than the old.

Continuing in this way we must eventually reach a stage where $A' = I$. Then we have

$$\begin{aligned} A \cdot W &= D_k \cdot W \cdot B' \\ &= (D_k \cdot W \cdot C_2 \cdot C_3 \cdots C_k \cdot C_1 \cdot C_2 \cdots C_{k-1}) \\ &\qquad \cdot C_{k-1} \cdots C_2 \cdot C_1 \cdot C_k \cdots C_3 \cdot C_2 \cdot B' && \text{by I} \\ &= W_k \cdot C_{k-1} \cdots C_2 \cdot C_1 \cdot C_k \cdots C_3 \cdot C_2 \cdot B' && \text{by def.} \end{aligned}$$

which is of the form $W_k \cdot B$.

The proof of the lemma now follows. Let the given expression be of the form

$$A_q \cdot W \cdot A_{q-1} \cdot W \cdots A_2 \cdot W \cdot A_1 \cdot W \cdot A_0 \tag{4}$$

where $A_0, A_1, A_2 \cdots A_q$ involve the C's only. By what we have just proved,

$$\begin{aligned} A_q \cdot W &= W_{k_q} \cdot B_q \cdot \\ B_q \cdot A_{q-1} \cdot W &= W_{k_{q-1}} \cdot B_{q-1} \\ B_{q-1} \cdot A_{q-2} \cdot W &= W_{k_{q-2}} \cdot B_{q-2} \\ \cdot \quad \cdot \quad \cdot \quad &\cdot \quad \cdot \quad \cdot \quad \cdot \\ B_2 \cdot A_1 \cdot W &= W_{k_1} \cdot B_1 \\ B_1 \cdot A_0 &= B. \end{aligned}$$

Taking all these into consideration, we can reduce the form (4) to the form (3). □

Lemma 2. *Every expression in* $\mathfrak{A}$ *can be reduced further to a form* (3), *in which*

$$k_q \geqq k_{q-1} \geqq \cdots\cdots \geqq k_2 \geqq k_1$$

Proof.

It is sufficient to prove that

$$W_j \cdot W_{k+1} = W_k \cdot W_j \qquad \text{for } k \geqq j. \tag{5}$$

The proof of (5) is as follows. □

First,

$$W_1 \cdot W_2 = W_1 \cdot W_1. \tag{6}$$

For

$$\begin{aligned} W_1 \cdot W_2 &= W_1 \cdot C_1 \cdot W_1 \cdot C_2 \cdot C_1 && \text{by def.} \\ &= W_1 \cdot W_1 && \text{by V and VI.} \end{aligned}$$

Second,

(7) $$W_1 \cdot W_{k+1} = W_k \cdot W_1 \quad \text{for } k > 1.$$

For
$$\begin{aligned} W_1 \cdot W_{k+1} &= W_1 \cdot D_{k+1} \cdot W_1 \cdot [3, 4, \cdots k+2, 1, 2] && \text{by def.} \\ &= D_k \cdot W_1 \cdot [3, 1, 2] \cdot W \cdot [3, 4, 1, 2] \\ &\qquad \cdot [3, 4, \cdots k+2, 1, 2] && \text{by VII.} \end{aligned}$$

But since
$$[3, 4, 1, 2] \cdot [3, 4, \cdots k+2, 1, 2] = [1, 2, 5, 6, \cdots k+2, 3, 4]$$

and
$$W_1 \cdot [1, 2, 5, 6, \cdots k+2, 3, 4] = [1, 4, 5, \cdots k+1, 2, 3] \cdot W_1 \quad \text{by IV.}$$
$$[3, 1, 2] \cdot [1, 4, 5, \cdots k+1, 2, 3] = [3, 4, \cdots k+1, 1, 2]$$

we have

$$\begin{aligned} W_1 \cdot W_{k+1} &= D_k \cdot W_1 \cdot [3, 4, \cdots k+1, 1, 2] \cdot W \\ &= W_k \cdot W_1 && \text{q. e. d.} \end{aligned}$$

Third,

(8) $$C_k \cdot W_j = W_j \cdot C_k \qquad \text{for } k < j - 1.$$

For by definition

$$C_k \cdot W_j = C_k \cdot D_j \cdot W \cdot [3, 4, \cdots j+1, 1, 2].$$

But we have

$$\begin{aligned} &C_k \cdot D_j = D_j \cdot C_{k+1} \\ &C_{k+1} \cdot W = W \cdot C_{k+2} \\ &C_{k+2} \cdot [3, 4, \cdots j+1, 1, 2] = [3, 4, \cdots j+1, 1, 2] \cdot C_k \end{aligned}$$

(the first and third relations follow from the known properties of permutations, the second from IV.) Combining these three we have (8).
Fourth,

(9) $$W_j \cdot C_j = W_j.$$

For $j = 1$, this is true by V.

Suppose, now, (9) is true for $j - 1$ (i. e. suppose $W_{j-1} \cdot C_{j-1} = W_{j-1}$) then

$$\begin{aligned} W_j \cdot C_j &= C_{j-1} \cdot W_{j-1} \cdot C_j \cdot C_{j-1} \cdot C_j && \text{by def.} \\ &= C_{j-1} \cdot W_{j-1} \cdot C_{j-1} \cdot C_j \cdot C_{j-1} && \text{by II.} \\ &= C_{j-1} \cdot W_{j-1} \cdot C_j \cdot C_{j-1} && \text{by hyp.} \\ &= W_{j-1} && \text{by def.} \end{aligned}$$

Fifth,

$$C_{j+h} \cdot W_j = W_j \cdot C_{j+h+1} \qquad \text{for } h > 0 \tag{10}$$

For $j = 1$, this is true by IV. Suppose it true for $j - 1$, then

$$\begin{aligned} C_{j+h} \cdot W_j &= C_{j+h} \cdot C_{j-1} \cdot W_{j-1} \cdot C_j \cdot C_{j-1} && \text{by def.} \\ &= C_{j-1} \cdot C_{j+h} \cdot W_{j-1} \cdot C_j \cdot C_{j-1} && \text{by III.} \\ &= C_{j-1} \cdot W_{j-1} \cdot C_{j+h+1} \cdot C_j \cdot C_{j-1} && \text{by hyp.} \\ &= C_{j-1} \cdot W_{j-1} \cdot C_j \cdot C_{j-1} \cdot C_{j+h+1} && \text{by III.} \\ &= W_j \cdot C_{j+h+1} \qquad \text{q.e.d.} && \text{by def.} \end{aligned}$$

Sixth,

For $j = 1$, this is true by (6). Suppose it true for $j - 1$, then

$$\begin{aligned} W_j \cdot W_j &= C_{j-1} \cdot W_{j-1} \cdot C_j \cdot W_{j-1} \cdot C_j \cdot C_{j-1} && \text{by def. and I.} \\ &= C_{j-1} \cdot W_{j-1} \cdot W_{j-1} \cdot C_{j+1} \cdot C_j \cdot C_{j-1} && \text{by (10)} \\ &= C_{j-1} \cdot W_{j-1} \cdot W_j \cdot C_{j+1} \cdot C_j \cdot C_{j-1} && \text{by hyp.} \\ &= C_{j-1} \cdot W_{j-1} \cdot C_j \cdot C_{j-1} \cdot C_{j-1} \cdot C_j \cdot W_j \cdot C_{j+1} \cdot C_j \cdot C_{j-1} && \text{by I.} \\ &= W_j \cdot C_{j-1} \cdot W_{j+1} \cdot C_{j-1} && \text{by def.} \\ &= W_j \cdot W_{j+1} \qquad \text{q.e.d.} && \text{by (8) and I.} \end{aligned}$$

Seventh,

$$W_j \cdot W_{k+1} = W_k \cdot W_j \qquad \text{for } k > j$$

For $j = 1$, this is true by (7). Suppose it true for $j - 1$, then,

$$\begin{aligned} W_k \cdot W_j &= W_k \cdot C_{j-1} \cdot W_{j-1} \cdot C_j \cdot C_{j-1} && \text{by def.} \\ &= C_{j-1} \cdot W_k \cdot W_{j-1} \cdot C_j \cdot C_{j-1} && \text{by (8), since } j-1 < k-1 \\ &= C_{j-1} \cdot W_{j-1} \cdot W_{k+1} \cdot C_j \cdot C_{j-1} && \text{by hyp.} \\ &= C_{j-1} \cdot W_{j-1} \cdot C_j \cdot C_{j-1} && \text{by (8)} \\ &= W_j \cdot W_{k+1} \qquad \text{q.e.d.} && \text{by def.} \end{aligned}$$

Definition: $W_k^r = W_k \cdot W_k \cdots W_k \quad r$ times.

Corollary. *Every expression in* $\mathfrak{A}$ *can be reduced to the form*

$$W_{k_q}^{r_q} \cdot W_{k_{q-1}}^{r_{q-1}} \cdots W_{k_2}^{r_2} \cdot W_{k_1}^{r_1} \cdot B \tag{11}$$

where $\quad k_q > k_{q-1} > \cdots\cdots > k_2 > k_1, \qquad r_1 > 0$

Proof. Simply collect the W's with equal indices in (3). □

Lemma 3. *If two expressions of the form* (11) *correspond to the same transformation, then they both have the same constants* $q, k_1, k_2, \cdots k_q, r_1 r_2, \cdots r_q$.

Proof.
Let

$$\Delta_q = W_{k_q}^{r_q} \cdot W_{k_{q-1}}^{r_{q-1}} \cdots W_{k_2}^{r_2} \cdot W_{k_1}^{r_1}$$

also let

$$\Delta_q \sim \alpha = [a_1, a_2, a_3 \cdots\cdots]$$

Then for the explicit determination of the a_x we have

$$\begin{array}{lrcl} \text{If} & 0 < x < k_1 & \text{then} & a_x = x \\ & k_1 \leqq x \leqq k_1 + r_1 & & a_x = k_1 \\ & k_1 + r_1 < x < k_2 + r_1 & & a_x = x - r_1 \\ & & \text{etc.} & \end{array}$$

In general, if we define

$$s_i = r_1 + r_2 + \cdots + r_1$$
$$r_0 = 0, s_0 = 0, k_0 = 0$$

then, for $i = 1, 2, \cdots q$.

$$\begin{array}{lrcl} \text{If} & k_{i-1} + s_{i-1} < x < k_i + s_{i-1} & \text{then} & a_x = x - s_{i-1} \\ & k_i + s_{i-1} \leqq x \leqq k_i + s_i & & a_x = k_i \\ & k_q + s_q < x & & a_x = x - s_q. \end{array}$$

These formulas follow directly from (1) and (2); their proofs are left to the reader.

The transformation has thus the following character: 1) the integers in the symbol $[a_1, a_2, a_3 \cdots]$ are arranged in their natural order with certain repetitions,

2) the only integers which appear more than once are $k_1, k_2 \cdots k_q$, and these appear respectively $r_1 + 1, r_2 + 1, \cdots r_q + 1$ times.
Now if $\beta = [b_1, b_2 \cdots]$ corresponds to B, then the transformation corresponding to $\Delta_q \cdot B$ is $\alpha \cdot \beta = [a_{b_1}, a_{b_2}, \cdots]$. By the restrictions on B the sequence $[a_{b_1}, a_{b_2}, \cdots]$ is merely a rearrangement of the sequence $[a_1, a_2 \cdots]$. Hence the second of the above properties applies just as much to $\alpha \cdot \beta$ as to α. But then the constants $q, k_1 \cdots k_q, r_1 \cdots r_q$, are uniquely determined by $\alpha \cdot \beta$. □

Lemma 4. *To each transformation of finite order there corresponds at least one expression of form* (11).

Proof.

Let the given transformation be $\gamma = [c_1, c_2 \cdots]$.

Let Δ_q be determined from γ as indicated in the preceding lemma, and suppose $\Delta_q \sim [a_1, a_2 \cdots] = \alpha$.

Then we can construct a permutation $\beta = [b_1, b_2 \cdots]$ such that $\alpha \cdot \beta = \gamma$, as follows. If c_i is distinct from any of the k's there is one and only one j such that $a_j = c_i$; in that case we must let $b_i = j$. On the other hand let the C's which are equal to k_j be $c_{i_1}, c_{i_2} \cdots c_{i_p}$ (where $p = r_j + 1$); then set $b_{i_1} = k_j + s_{j-1}, b_{i_2} = b_{i_1} + 1, b_{i_3} = b_{i_2} + 1$, etc. For definiteness we may suppose that $i_1 < i_2 < \cdots < i_p$. Then $\alpha \cdot \beta = \gamma$; for the i'th integer in the symbol for $\alpha \cdot \beta$ is a_{b_i}, and b_i has been so chosen that in all cases $a_{b_i} = c_i$.

To the β so constructed there corresponds a unique B in $\mathfrak{A}$, by Moore's result. For this B, $\Delta_q \cdot B \sim \gamma$. □

Lemma 5. *The operator in $\mathfrak{A}$ corresponding to a given transformation is unique.*

Proof.

Let A_1 and A_2 be two operators in $\mathfrak{A}$ which correspond to a given transformation γ. By Lemmas 2 and 3 there is a uniquely determined Δ_q such that

$$A_1 = \Delta_q \cdot B_1, \qquad A_2 = \Delta_q \cdot B_2$$

If $B_1 \sim \beta_1, B_2 \sim \beta_2, \beta_1$ and β_2 must be subject to all the restrictions to which β was subject in Lemma 4, except that it is not necessary to suppose $i_1 < i_2 < \cdots < i_p$. The only way in which β_1 and β_2 can differ is in the arrangement of the $b_{i_1}, b_{i_2} \cdots$ corresponding to each of the k_j. Hence

$$\beta_2 = \beta_3 \cdot \beta_1$$

where β_3 is a product of permutations, each of which permutes among them selves the integers composing one of the sets $k_j + s_{j-1}, k_j + s_{j-1} + 1, \cdots k_j + s_j$.

Let us now agree to denote by $E_i^j, i < j$ a combinations of $C_i, C_{i+1} \cdots C_{j-1}$ (corresponding to a permeation of $i, i+1, \cdots j$). Then, in view of the isomorphism already established by Moore, we have the following result; there exists a B_3 such that

$$B_2 = B_3 \cdot B_1$$
$$B_3 = E_{k_1}^{k_1+r_1} \cdot E_{k_2+s_1}^{k_2+s_2} \cdot E_{k_3+s_2}^{k_3+s_3} \cdots E_{k_q+s_{q-1}}^{k_q+s_q}$$

To prove the lemma it is sufficient to show that $\Delta_q \cdot B_3 = \Delta_q$. This, in turn, follows from the above form for B_3, if we demonstrate that

$$\Delta_h \cdot E_{k_h+s_{h-1}}^{k_h+s_h} = \Delta_k \qquad (h = 1, 2, \cdots, q). \tag{12}$$

We turn to this last question forthwith.

In the first place, if

$$i > k+1, W_k \cdot E_i^j = E_{i-1}^{j-1} \cdot W_k.$$

This follows from (10), under Lemma 2.

Next, if $i > k+1$

$$W_k^r \cdot E_i^j = E_{i-r}^{j-r} \cdot W_k^r. \tag{13}$$

This is derived from the preceding by induction on r.

Third, if $i < h$

$$\Delta_i \cdot E_{k_h+s_{h-1}}^{k_h+s_h} = E_{k_h+s_{h-1}-s_i}^{k_h+s_h-s_i} \cdot \Delta_i. \tag{14}$$

For $i = 1$, this follows from the preceding, for the conditions $k_h + s_{h-1} > k_1 + r_1$ are satisfied since, if $h > 1$, $k_h > k_1$, $s_{h-1} \geqq s_1 = r_1$. For $i > 1$ we prove (14) by induction. Suppose it true for $i - 1$, then,

$$\begin{aligned} \Delta_i \cdot E_{k_h+s_h}^{k_h+s_{h-1}} &= W_{k_i}^{r_i} \cdot \Delta_{i-1} \cdot E_{k_h+s_{h-1}}^{k_h+s_h} \\ &= W_{k_i}^{r_i} \cdot E_{k_h+s_{h-1}-s_{i-1}}^{k_h+s_h-s_{i-1}} \cdot \Delta_{i-1}. \end{aligned}$$

In order, now, to apply (13), we need to know simply that

$$k_h + s_{h-1} - s_{i-1} > k_i + r_i$$

and this is fulfilled since for $h > i$,

$$s_{h-1} - s_{i-1} = r_i + r_{i+1} + \cdots + r_{h-1} \geqq r_i.$$

Hence

$$W_{k_i}^{r_i} \cdot E_{k_h+s_{h-1}-s_{i-1}}^{k_h+s_h-s_{i-1}} \cdot \Delta_{i-1} = E_{k_h+s_{h-1}-s_i}^{k_h+s_h-s_i} \cdot W_{k_i}^{r_i} \cdot \Delta_{i-1}$$

so that (14) is proved.

The following is the special case of (14) where $i = h - 1$

$$\Delta_{h-1} \cdot E_{k_h+s_{h-1}}^{k_h+s_h} = E_{k_h}^{k_h+r_h} \cdot \Delta_{h-1}.$$

In order to complete the proof of (12), it remains (since $\Delta_h = W_{k_h}^{r_h} \cdot \Delta_{h-1}$) simply to show

$$W_{k_h}^{r_h} \cdot E_{k_h}^{k_h+r_h} = W_{k_h}^{r_h} \tag{15}$$

In view of the composition of $E_{k_h}^{k_h+r_h}$, (15) follows from

$$W_k^r \cdot C_{k+j} = W_k^r \qquad \text{for } 0 \leqq j < r.$$

For $j = 0$, this is true by (9), under Lemma 2. For $j = 1$

$$\begin{aligned} W_k \cdot W_k \cdot C_{k+1} &= W_k \cdot W_{k+1} \cdot C_{k+1} && \text{by (5)} \\ &= W_k \cdot W_{k+1} && \text{by (9)} \\ &= W_k \cdot W_k && \text{by (5)} \\ \therefore \quad W_k^r \cdot C_{k+1} &= W_k^r && \text{for } r \geqq 2. \end{aligned}$$

For $j > 1$, let $r = s + j - 1$, then $s \geqq 2$ and

$$\begin{aligned} W_k^r \cdot C_{k+j} &= W_k^s \cdot W_k^{j-1} \cdot C_{k+j} \\ &= W_k^s \cdot C_{k+1} \cdot W_k^{j-1} && \text{by (10)} \\ &= W_k^s \cdot W_k^{j-1} && \text{by the previous case} \\ &= W_k^r. \end{aligned}$$

These three cases together establish (15), which completes the proof of both the lemma and the theorem. □

□

We have now achieved one of our objectives—viz. the elimination of Rule 4 so far as the selected subclass is concerned. For Rule 4 merely enables us to conclude that two entities of the subclass, whose application to a series $x_0 x_1 x_2 \cdots$ yields the same transformation, are equal. These entities correspond to the same transformation in the sense of our theorem, and therefore by that theorem are equal. Moreover the proof of the theorem is such that in any particular case a proof of the equality can be constructed in terms of I-VII, together with the rules for identity and no more. This proof will in general be quite long, but it may nevertheless be found.*

Finally we have an analysis of substitution in so far as that process is equivalent to transformation.

There remain open two questions: 1) What is the relation between the transforms of a function of $n-1$ variables, obtained by substituting a constant in a function of n variables, and the transforms of the original; 2) How can our infinite set of postulates be reduced to a finite set. Both these questions can be answered by introducing the entity B defined in Part II. But when we do that, it is expedient to consider a more extensive subclass. This takes us out of the domain of simple substitution. The topic is left for a later paper.

* MISSING FOOTNOTE IN ORIGINAL PAPER