ON THE EXISTENCE OF LINEAR ALGEBRAS IN BOOLEAN ALGEBRAS*

BY ORRIN FRINK, JR.†

According to the definition to be found in Dickson's *Algebras and their Arithmetics*, pages 9–11, the following properties are characteristic of a linear algebra.

(1) *The elements of the algebra form an abelian group with respect to addition.*

(2) *Multiplication is distributive with respect to addition.*

(3) *The algebra has a finite basis*; *that is, a finite number of elements can be found such that every element of the algebra can be expressed as a linear combination of these basal units, with coefficients taken from the field over which the algebra is defined.*

With this definition in mind we wish to determine for what pairs of Boolean operations considered as the addition and multiplication operations the elements of a Boolean algebra will constitute a linear algebra. We are limited in our choice of an addition operation by the first property above to operations of the form $axy+a'xy'+a'x'y+ax'y'$, which Bernstein‡ has shown to be the only Boolean abelian group operations. To find suitable multiplication operations $pxy+qxy'+rx'y+sx'y'$, we seek those which are distributive with respect to the above. The condition that the first distributive law hold is found in Schröder's *Algebra der Logik* (vol. 2, p. 503) to be

$$a'(pq+rs)+(ad+a'd'+bc+b'c')(p'q+r's)+d(p'q'+r's')=0,$$

where a, b, c, d, and p, q, r, s are the discriminants of the addition and multiplication operations respectively. Here $a=d$, and $b=c=a'$; hence we get $p'q=r's=a'q=a's=ap'$

* Presented to the Society, January 1, 1926.

† National Research Fellow.

‡ Transactions of this Society, vol. 26, p. 174.

$=ar'=0$, which can be written $p>a>q$, $r>a>s$. Similarly from the second distributive law we get $p>a>r$, and $q>a>s$. It follows that $q=r=a$, whence it is seen that multiplication must be commutative. Our multiplication operations then must be of the form $pxy+axy'+ax'y+sx'y'$, where $p>a>s$. Another way of writing this which involves only two parameters is $(a+b)xy+axy'+ax'y+ab'x'y'$, where $b=ps'$. It is to be noted that these operations are all associative, the condition being $p's+(p'+s)(qr'+q'r)=0$.

Before trying to satisfy the condition about the finite basis, we will look for *idempotent* elements, that is, elements e not equal to a such that $e^2=e$. Setting $y=x$ in the multiplication operation gives us $(a+b)x+ab'x'$. Equating this to x, we conclude that x is idempotent when and only when it is of the form $(a+b)u+ab'u'$, where u is arbitrary. On the other hand, an element n not equal to a such that $n^2=a$ is *nilpotent.* Equating the above expression for x^2 to a we see that all elements of the form $(a+b')u+abu'$ are nilpotent. If we substitute this expression for a nilpotent element in the multiplication operation we also see that the product of one of these nilpotent elements by any element of the algebra is a. Of course it should be remembered that a corresponds to zero in our algebra.

An important fact is that any element of the algebra can be expressed as the "sum" of an idempotent element and a nilpotent element. For we have $x=(ab'+xb)\oplus(ab+xb')$, where the sign $\oplus$ represents our addition operation as distinguished from logical addition. This is an illustration of the principal theorem on algebras (Dickson, loc. cit., p. 125), which states that any associative linear algebra is the sum of its maximum invariant nilpotent sub-algebra and a semi-simple algebra. The sum is here a direct sum, the cross products being zero.

In our case the field over which the algebra is supposed to be defined is not given to us in advance, as contemplated by the definition of linear algebras. However, an algebra which contains an idempotent element must contain a sub-algebra which is isomorphic with the field. It can be seen that a and any idempotent e form a field of 2 elements. Bernstein[*] has shown that the only possible fields in Boolean algebras are of this kind, and in fact if a field contained besides a and e another element f, then since f^2 is idempotent it would have to equal e, since a field cannot contain two idempotents. In that case, however, $e \oplus f$ would be nilpotent, which is likewise impossible in a field. Since we are limited to finite fields, we see that if our algebra is to have a finite basis it must itself be finite. However, any Boolean algebra contains finite Boolean sub-algebras, and hence may contain linear algebras.

We have seen that our entire algebra is the direct sum of a zero algebra and an idempotent algebra. If either b or b' contains only a finite number of elements, then one of these two sub-algebras is finite and may have a finite basis. Suppose the idempotent algebra is finite and contains exactly 2^n elements of the form $ab'+kb$. The product of two such elements $ab'+xb$ and $ab'+yb$ is seen to be $ab'+(xy+axy'+ax'y)b$. We see from this that we may set up a correspondence which is preserved under multiplication, between the elements $ab'+kb$ of our idempotent algebra and the elements kb of a Boolean algebra[†] whose multiplication operation is $xy+axy'+ax'y$. This Boolean algebra can be represented by the subsets of a set of n elements $(e_1, e_2, \cdots, e_n)$, which combine under logical addition and multiplication. We now pick out the elements kb corresponding to the unit sets (e_1), (e_2), $\cdots$, (e_n) and call them k_1b, k_2b, $\cdots$, k_nb. We then choose as basal units for the idempotent algebra the elements $ab'+k_ib$ $(i=1, 2, \cdots, n)$. The product of any two of these is a if they are distinct. Our field consists of the two elements a and $ab'+a'b$, the latter being the modulus of the algebra. It is seen that these elements correspond to the null set and the universal set

[*] Transactions of this Society, vol. 28 (1926), p. 654.

[†] N. Wiener, Transactions of this Society, vol. 18 (1917), p. 65.

in the above representation by means of subsets. To see how an element x of the linear algebra is represented as a linear combination of the basal units, we merely find to what subset of $(e_1, e_2, \cdots, e_n)$ x corresponds. The subscripts of the k's which appear in the linear combination are the same as those of the e's which appear in the subset.

No particular difficulty presents itself in picking a set of basal units for the zero algebra if it is finite. The elements form an abelian group with respect to addition, of order say 2^m, and we need merely select a set of m generators of the group for our basal units. The field, of order 2, must be taken outside the algebra, since the latter does not have a modulus. If the entire algebra is finite, in choosing a set of basal units for it we select the units for the sub-algebras separately, and again we must consider the field to be outside the algebra, since it has no modulus if the nilpotent part exists.

We may sum up our results thus far as follows.

The elements of a Boolean algebra form for the operations $axy+a'xy'+a'x'y+ax'y'$ *and* $(a+b)xy+ax'y+axy'+ab'x'y'$ *considered as the addition and multiplication operations respectively a commutative associative algebra which is the direct sum of a zero algebra and an algebra all of whose elements except the zero element are idempotent. If either of these sub-algebras is finite, it may be represented as a linear algebra over* $GF(2)$, *as may the entire algebra if it is finite.*

These results I consider important for Boolean algebra and the algebra of classes. Let $a=0$ and $b=1$, which gets rid of the zero algebra. Then our addition and multiplication operations become $xy'+x'y$ and xy respectively. In other words we may substitute the operation $xy'+x'y$ for logical addition in Boolean algebra. This operation, which I will for the time being represent with Peano by $x \circ y$, has been treated by many authors, but to Veblen* belongs the credit for introducing it as the addition operation to replace

* Cambridge Colloquium Lectures, p. 9.

logical addition. In the analysis situs applications, where it is called "addition modulo 2," it plays a more important role than logical addition, and its use results in formulas which resemble more those of ordinary algebra.

Two important properties of this operation are $a \oplus a = 0$, and $a' \circ a = 1$ for all values of a. From the first it follows that we may transpose terms from one side of an equation to the other. In virtue of the second property we can avoid entirely the use of the Boolean negation x'. Another important fact is that logical addition and addition modulo 2 are interchangeable when there is no overlapping between terms, as for example in the case of a Boolean expression in the completely expanded form. Thus consider a Boolean function of two variables $f(x, y) = axy + bxy' + cx'y + dx'y'$. Here we could substitute $\circ$ for $+$. If we wish to avoid the use of the negation sign we replace x' by $x \circ 1$ and y' by $y \circ 1$, obtaining $f(x, y) = pxy \circ qx \circ ry \circ d$, where $p = a + b + c + d$, $q = b + d$, and $r = c + d$. This may be considered the normal form for a function of two variables written in terms of addition modulo 2. To pass from an expression of the latter type to one involving logical addition, we may use the well known rule for obtaining the discriminants of a Boolean expression by giving the variables the values 0 and 1. As a final remark it is interesting to note that although we may speak of the logical sum of an infinite number of elements, the sum modulo 2 of an infinite number of elements is in general meaningless.

Princeton University