19. On Postulate-Sets for Newman Algebra and Boolean Algebra. I

By Yuki WOOYENAKA
Japan Women's University, Tokyo
(Comm. by Kinjirô KUNUGI, M.J.A., Feb. 12, 1964)

Introduction. There are many sets of postulates for Boolean algebra given by various scholars [1]. Moreover, M. H. Stone has shown among other things, that one can subsume the theory of Boolean algebra under the theory of Boolean ring [2]. The sets of postulates for Boolean ring (or generalized Boolean algebra) were given by Stabler [3] and Bernstein [4]. On the other hand, Newman has given the most remarkable system known as Newman algebra [5, 6] including both Boolean algebra and Boolean ring.

We shall give in this paper two kinds of postulate-sets for Newman algebra as Set I and Set II. The idea of the postulates of Set I was suggested to me by Bernstein's dual-symmetric definition of Boolean algebra [7] where the distributive law $a\vee(bc)=(a\vee b)(a\vee c)$ is eliminated. In Set II, we have replaced the commutative laws for addition and multiplication by axioms B_1', C', and C_1' below. This set has not an exactly dual, but a nearly dual form. And this set has a form quite close to that of the postulates of Newman algebra due to Birkhoff: our axioms B_1, B_1' are just the same as the axioms N1, N1′ of Birkhoff [6: p. 155], our C_1', C_1 are nearly like N2, N3, and our E' corresponds to N4.

The paper consists of three paragraphs. The first gives the postulates of Set I and Set II and shows that each set is equivalent with the system of Newman algebra [6]. Four kinds of postulate-sets for Boolean algebras, Set I_1, Set I_2^*, Set II_1, and Set II_2^* will be derived from Set I and Set II respectively by Newman's decomposition theorem. The second deals with the construction of some independence-systems with eight elements. In constructing these systems we give several theorems where we shall see how helpful Stone's theory of Boolean ring [2] will also be for our purpose. The third gives the independence proofs for the four new sets for Boolean algebras.

In concluding, we should like to give the following remark. G. D. Birkhoff and G. Birkhoff say in the introduction of their paper, that they have made Newman's argument such shorter and simpler in adding a dependent postulate $0+a=a$. Our Sets I and II are independent sets and fit for Birkhoff's argument. As such our sets may be regarded as one of the suitable systems to characterize

Newman algebra.

1. Sets I and II. The postulates of sets I and II are the propositions below on a *class* K, *two binary operations* $+$, $\times$ and a *unary operation* $'$ (in the postulates that are not existence postulates supply the restriction: *if the elements indicated are in* K).

It will be noted that in the present sets we shall replace Bernstein's "$\vee$" by "$+$", and for the sake of brevity we shall write ab for $a\times b$, and moreover, name the postulates A, A_1 etc. after Bernstein [7]. It is also to be remarked in our postulate E$'$ on the unary operation $'$, the uniqueness of a' is not required (in spite of the usual definition of the "unary operation"). This uniqueness will be deduced from the other postulates.

Set I

F$'$. K is not empty.

D. If $a, b\in K$, then an element $a+b\in K$ is uniquely determined.

D_1. If $a, b\in K$, then an element $ab\in K$ is uniquely determined.

E$'$. To every $a\in K$ corresponds at least one $a'\in K$.

A. $a+b=b+a$.

A_1. $ab=ba$.

B_1. $a(b+c)=ab+ac$.

C. $a+b'b=a$.

C_1. $a(b'+b)=a$.

Set II

F$'$, D, D_1, E$'$, B_1 as mentioned above.

B_1'. $(a+b)c=ac+bc$.

C$'$. $a+b'b=b'b+a=a$.

C_1'. $a(b'+b)=(b'+b)a=a$.

It is easy to see that the Newman algebra according to Birkhoff's definition[6] satisfies the postulates of Set I as well as of Set II.

Now it remains to show that the postulates of Newman algebra can be deduced from Set I and Set II respectively. This is shown by the following theorems. In the proofs of these theorems we shall enumerate the names of postulates B_1, C$'$, etc. used in the transformation of formulas. If more than one postulates, e.g. B_1 and C$'$ are used in one step, we shall write B_1-C$'$. The use of postulates F$'$, D, D_1, and E$'$ will be implicit, except for six cases where they are noted for emphasis.

Theorem 0. $(a')'=a$ for all a and all $(a')'$.

(We write a'' for $(a')'$ for the sake of brevity.)

Proof. $a''=a''(a'+a)=a''a'+a''a=a''a+a'a=(a''+a')a=a$ by C_1, B_1, A-C-C, B_1-A_1, A_1-C_1 in Set I, and by C_1', B_1, C$'$-C$'$, B_1', C_1' in Set II.

Theorem 1. a' is uniquely determined.

Proof. Let a_1' and a_2' be two elements corresponding to a by

operation $'$ (by E$'$), then
$a_1'=a_1'(a_2'+a)=a_1'a_2'+a_1'a=a_1'a_2'=a_1'a_2'+(a_2')'a_2'=(a_1'+(a_2')')a_2'=(a_1'+a)a_2'=a_2'$ by C_1, B_1, C, C, B_1-A_1, Theorem 0, A_1-C_1 in Set I, and by C_1', B_1', C$'$, C$'$, B_1', Theorem 0, C_1' in Set II.

Theorem 2. $a+a'=a'+a=b'+b$ for any $a, b\in K$, thus the element $a+a'=a'+a$ does not depend on a.

Proof. For Set I: $a+a'=a'+a=(a'+a)(b'+b)=(b'+b)(a'+a)=b'+b$ by A, C_1, A_1', C_1 and E$'$-Theorem 1-D.

For Set II: $a+a'=(a''+a')(a'+a)=a'+a=(b'+b)(a+a')=b'+b$ by Theorem 0-C$'$, C_1', C_1', C_1', and E$'$-Theorem 1-D.

Definition 1. This element $a'+a=a+a'$ is denoted by 1.

Theorem 2_1. $aa'=a'a=b'b$ for any $a, b\in K$, thus the element $aa'=a'a$ does not depend on a.

Proof. For Set I: $aa'=a'a=a'a+b'b=b'b+a'a=b'b$ by A_1, C, A, C and E$'$-Theorem 1-D_1.

For Set II: $aa'=a''a'+a'a=a'a=a'a+b'b=b'b$ by Theorem 0-C$'$, C$'$, C$'$, C$'$ and E$'$-Theorem 1-D_1.

Definition 2. This element $a'a=aa'$ is denoted by 0.

Theorem 3. $\exists 1,\quad a1=a$.

Proof. This follows from C_1-Definition 1 in Set I and from C_1'-Definition 1 in Set II.

Theorem 4. $\exists 0,\quad a+0=0+a=a$.

Proof. This follows from C-Definition 2 in Set I and from C$'$-Definition 2 in Set II.

Theorem 5. $\exists a',\quad a+a'=1$ and $aa'=0$.

Proof. This follows from E$'$, Definition 1, Definition 2 in both Sets I and II.

Thus we come to the conclusion that each of these sets, Set I and Set II, is equivalent to the postulates of Newman algebra.

The Newman algebra K is, as is well known, decomposed into the direct union of two subalgebras K_1, K_2 consisting respectively of "even"- and "odd"-elements. K_1 is a Boolean algebra and K_2 satisfies all postulates for the Boolean ring with unity as given by Stone [2: p. 39] except the associativity of multiplication. The following example of Newman algebra shows that K_2 can be really non-associative.

$+$	0	1	a	b	c	α	β	γ
0	0	1	a	b	c	α	β	γ
1	1	0	α	β	γ	a	b	c
a	a	α	0	γ	β	1	c	b
b	b	β	γ	0	α	c	1	a
c	c	γ	β	α	0	b	a	1
α	α	a	1	c	b	0	γ	β
β	β	b	c	1	a	γ	0	α
γ	γ	c	b	a	1	β	α	0

$\times$	0	1	a	b	c	α	β	γ
0	0	0	0	0	0	0	0	0
1	0	1	a	b	c	α	β	γ
a	0	a	a	1	1	0	α	α
b	0	b	1	b	1	β	0	β
c	0	c	1	1	c	γ	γ	0
α	0	α	0	β	γ	α	γ	β
β	0	β	α	0	γ	γ	β	α
γ	0	γ	α	β	0	β	α	γ

a	a'
0	1
1	0
a	α
b	β
c	γ
α	a
β	b
γ	c

We shall call an algebra satisfying all postulates for the Boolean ring with unity except the associative law for multiplication a *quasi-Boolean ring*, and by a *generalized quasi-Boolean ring* we shall mean an algebra which satisfies all postulates for the Boolean ring except for the associative law for multiplication, the existence of unity not being required.

Theorem 6. If $a+a=0$ holds for every element a of Newman algebra, then $(a'+a)+a=a'$ also holds for every a and every a' of this Newman algebra. The converse also holds. When each of these conditions holds then the Newman algebra is a quasi-Boolean ring.

Proof. It is known that if $a+a=0$ holds identically in a Newman algebra, this Newman algebra is a quasi-Boolean ring [5]. Therefore we have $(a'+a)+a=a'+(a+a)=a'+0=a'$. Conversely, if $(a'+a)+a=a'$ holds identically in a Newman algebra, then we have $0=a'a=\{(a'+a)+a\}a=(a'+a)a+aa=(a'a+aa)+a=(0+a)+a=a+a$ [6].

Starting from our sets I and II, we obtain by the direct decomposition theorems [6] and by Theorem 6 the following sets I_1, II_1 for the Boolean algebra and I_2, II_2 for the quasi-Boolean ring:

Set I_1: F′, D, D_1, E′, A, A_1, B′, B_1, C, C_1.

Set II_1: F′, D, D_1, E′, B′, B_1, B_1', C′, C_1'.

Set I_2: F′, D, D_1, E′, A, A_1, B_1, C, C_1, G.

Set II_2: F′, D, D_1, E′, B_1, B_1', C′, C_1', G.

where B′, G mean the following postulates:

B′. $a+a=a$.

G. $(a'+a)+a=a'$.

If we add to Set I_2 and Set II_2 the postulate of the associativity

H. $(aa)b=a(ab)$ [4]

respectively, then we obtain the postulate-sets for the Boolean ring with unity. We shall denote these postulate-sets I_2^*, II_2^* respectively.

2. On the construction of some independence-systems. We shall give in the following paragraph 3 the independence proofs of each postulate in Set I_1, Set II_1, Set I_2^*, Set II_2^* respectively. These proofs may be given by simple independence systems with at most four elements, except for the postulates A_1, B_1, B_1', H for which eight-element systems are needed. In this paragraph, we shall show that these relatively complicated systems can be constructed in more or less systematic manners.

Theorem 7. If the associative law for multiplication holds in a finite generalized quasi-Boolean ring R, then R has a unit.

Proof. If the associative law for multiplication holds in a finite generalized quasi-Boolean ring R, then it is evident from the definition that R is a finite Boolean ring. Let $a_1, a_2, \cdots, a_N$ be all the elements of R. Then it is easy to see that the sum of N elementary symmetric functions of $a_1, a_2, \cdots, a_N$ is a unit of R [2: p. 42]. Thus the theorem is proved.

Definition 3. We shall call an element a of a generalized quasi-Boolean ring R "a strong zero-devisor in R" if $a \neq 0$ and there exists an element $b \neq 0$ of R such that $ab=0$ or $ba=0$.

Theorem 8. If the associative law for multiplication holds in a finite generalized quasi-Boolean ring R with more than two elements, then R contains a strong zero-divisor.

Proof. By Theorem 7 R is a finite Boolean ring with unit, and the cardinal number of R is 2^n [2], the unit will be denoted as 1. R has an element a such that $a \neq 0$ and also $a \neq 1$, then we have $a+1 \neq 0$ and $a(a+1)=aa+a1=a+a=0$. Thus a is a strong zero-divisor and the theorem is proved.

Theorem 9. The cardinal number N of a finite non-associative generalized quasi-Boolean ring R is a power of 2, 2^m $(m \geqq 2)$.

Proof. R forms an additive abelian group of N elements in which $a+a=0$ holds for any element a. Therefore we can follow the proof which was given by Stone [2: pp. 42–43], and the condition $m \geqq 2$ results from the non-associativity.

Theorem 10. Every generalized quasi-Boolean ring R can be imbedded in a quasi-Boolean ring S, in such a manner that S is unique in the following sense: if T is a quasi-Boolean ring containing R, then T contains also a quasi-Boolean ring S^* isomorphic to S and containing R.

Proof. Of cause in discussing the possibility of imbedding a generalized quasi-Boolean ring R in a quasi-Boolean ring S we may disregard the trivial case where R has a unit and S coincides with R. We first provide an abstract element ε, distinct from those of R, and define

$$\varepsilon\varepsilon=\varepsilon, \quad \varepsilon a=a\varepsilon=a, \quad \varepsilon+0=0+\varepsilon=\varepsilon, \quad \varepsilon+\varepsilon=0,$$

0 being the zero element and a any element of R. We observe that the elements 0 and ε constitute a two-element Boolean ring I. Now we let S the direct union $R \times I$ of pairs (a, α) where $a \in R$, $\alpha \in I$ and $\alpha=0$ or $\alpha=\varepsilon$, defining the equality of (a, α) and (b, β) as $a=b$ and $\alpha=\beta$. We define the operations of addition and multiplication in S by

$$(a, \alpha)+(b, \beta)=(a+b, \alpha+\beta),$$
$$(a, \alpha)(b, \beta)=(ab+\alpha b+a\beta, \alpha\beta).$$

It is easily verified that under these operations the class S of pairs (a, α) is a quasi-Boolean ring with $(0, \varepsilon)$ as unit. To prove the uniqueness of S we can follow the proof of Stone for his Theorem 1 [2: pp. 40–42], as the associative law for multiplication in R is used only to show that the same law holds in S.

Now let us try to construct a non-associative generalized quasi-Boolean ring. If such a ring exists, it has by Theorem 9 a cardinal number 2^m, $m \geqq 2$, and the addition group of the type $(2, 2, \cdots, 2)$. So, if we construct such a ring with four elements, it is a "smallest" one in the sense that it can not have any proper subring with the same property. On the other hand, by Theorems 7 and 8 a generalized quasi-Boolean ring without a unit or without a strong zero-divisor is necessarily non-associative. Now we have the following example of a generalized quasi-Boolean ring with four elements without unit and without a strong zero-divisor:

$+$	0	α	β	γ
0	0	α	β	γ
α	α	0	γ	β
β	β	γ	0	α
γ	γ	β	α	0

$\times$	0	α	β	γ
0	0	0	0	0
α	0	α	γ	β
β	0	γ	β	α
γ	0	β	α	γ

Thus we have an example of "smallest" non-associative generalized quasi-Boolean ring. We shall denote this ring with R. Applying Theorem 10 to this R, we obtain system S of eight elements (already shown in the preceding paragraph) which forms a non-associative quasi-Boolean ring. It is easy to see that the quasi-Boolean ring satisfies the postulates of Newman algebra, therefore we can use this example for the independence proof of postulate H in Set I_2^* and Set II_2^* respectively.