*Indian J. pure appl. Math.*, **11**(10) : 1286–1292, October 1980

# SOME NUMBER THEORETIC BOOLEAN RINGS

J. HANUMANTHACHARI

*Department of Mathematics, S. V. U. College, Tirupati* 517502

(*Received* 23 *October* 1978; *after revision* 26 *May* 1980)

The aim of this paper is to find a necessary and sufficient condition for a set of divisors of a given positive integer $N$ to form a Boolean ring with respect to the operations $\oplus$ and $\odot$ defined by

$$a \oplus b = ([a, b], [N/a, N/b])$$

$$a \odot b = (a, b),$$

where $a, b$ are any two divisions of $N$ and $[a, b]$, $(a, b)$ denote the least common multiple (lcm) and the greatest common divisor (gcd) of $a, b$ respectively.

Also a new convolution of arithmetic functions is studied.

## 1. INTRODUCTION

An element $p$ of a ring is said to be idempotent if $p^2 = p$. A Boolean ring is a ring with identity in which every element is idempotent.

Halmos (1967, pp. 1–9) gave a number theoretic example of a Boolean algebra, viz., the set $\mathcal{D}_N$ of all divisors of a square-free integer $N$ with respect to the operations of forming the lcm and the gcd. We observe further that this set $\mathcal{D}_N$ will also form a Boolean ring with respect to the following special operations $\oplus$ and $\odot$, defined by

$$a \oplus b = ([a, b], [N/a, N/b])^{\dagger},$$

$$a \odot b = (a, b),$$

where $a, b$ are any two divisors of $N$ and $[a, b]$, $(a, b)$ denote the lcm and the gcd of $a, b$ respectively. It is natural to inquire whether, when $N$ is not a squarefree integer, any subset $C$ of $\mathcal{D}_N$ is a Boolean ring with respect to the above operations. The following example is an answer to this question in the affirmative:

(a) Let $N = 360$, $C = \{6, 12, 30, 60\}$. Then $\langle C, \oplus, \odot \rangle$ is a Boolean ring.

---

†This definition is another version of the usual formula for recovering the Boolean ring operations from those of the Boolean algebra. The usual formulation would be

$$a \oplus b = [(a, N/b), (b, N/a)].$$

In fact either of these is equal to $(ab, N)/(a, b)$.

(b) The set $\mathcal{CV} = \{1, 3, 5, 15\}$ of divisors of $N = 120$ is a Boolean ring with respect to the above special operations, $\oplus$ and $\odot$.

Hence our interest is to find a necessary and sufficient condition for a set $\mathcal{C}$ of divisors of a given positive integer $N$ to form a Boolean ring under the special operations. This we study in section 2. Next in section 3, we introduce the notion of an Arithmetic function and study a new product of these functions called Boolean convolution and examine some of its interesting properties.

## 2. A Necessary and Sufficient Condition for a Set of Divisors to Form A Boolean Ring

A divisor $d$ of $N$ is said to be unitary if $(d, N/d) = 1$. Henceforth, we let $\mathcal{C}$ a subset of $\mathcal{D}_N$, $\mathcal{U}$ the set of all unitary divisors of $N$ and $\mathcal{CV}$ a subset of $\mathcal{U}$.

*Theorem* 2.1 — If $N = \prod_{t=1}^{r} p_t^{\alpha_t}$, $a = \prod_{t=1}^{r} p_t^{\beta_t}$, $a \in \mathcal{C}$ and if

(1) $\mathcal{C}$ is closed with respect to $\oplus$ and $\odot$ ;

(2) $e = \prod_{t=1}^{r} p_t^{\epsilon_t}$ and $d = \prod_{t=1}^{r} p_t^{\delta_t}$ are the identities with respect to the special operations respectively; and

(3) $a \oplus a = e$, $\forall\ a \in \mathcal{C}$, then for every prime factor $p_t$ dividing $N$,

(i) $\beta_t \leqslant \delta_t$ (ii) $\beta_t = \epsilon_t$ or $\beta_t = \alpha_t - \epsilon_t$ (iii) $\epsilon_t \leqslant \alpha_{t/2}$ and $\epsilon_t \leqslant \beta_t$.

Proof: Since $d$ is an identity with respect to $\odot$, (i) follows immediately. (ii) is evident from (3). (iii) follows directly from (3), noting that

$$(a, N/a) = e \Rightarrow e \mid a \text{ and } e \mid N/a \Rightarrow \epsilon_t \leqslant \beta_t \text{ and } \epsilon_t \leqslant \alpha_t - \beta_t$$

*Illustrative Example* : Let $N = 2^3.3^2.7 = 504$,

$$e = 2.3 = 6,\ d = 2^2.3.7 = 84, \text{ and } \mathcal{C} = \{6, 12, 42, 84\}.$$

Then, $\langle \mathcal{C}, \oplus, \odot \rangle$ satisfies (1), (2) and (3) of Theorem 2.1. The members of $\mathcal{C}$ satisfy (i) to (iii) of the same.

*Note* : 1. From results (i) and (iii) we obtain

$$e \leqslant a \leqslant d,\ \forall\ a \in \mathcal{C}.$$

2. Further if $\mathcal{C}$ is Boolean ring with $e$ and $d$ as the respective identities with respect to the special operations, then conditions of Theorem 2.1 are satisfied and the results of Theorem 2.1 are, therefore true.

e.g. Let $N = 2^2.3.5 = 60$, $e = 2$, $d = 2.3.5 = 30$ and $C = \{2, 6, 10, 30\}$. Then $\langle C, \oplus, \odot \rangle$ is a Boolean ring. The elements of $C$ satisfy the conditions (i) to (iii) of Theorem 2.1.

3. Lastly, if $e = 1$, then every member of $C$ is a unitary divisor and so $C \subseteq \mathcal{U}$.

e.g : Let $N = 2^2.5 = 20$, $e = 1$, $d = 5$ and $C = \{1, 5\}$. Then $\langle C, \oplus, \odot \rangle$ satisfies (1), (2) and (3) of Theorem 2.1. The members of $C$ satisfy (i), (ii) and (iii) of the same theorem. In fact $C \subseteq \mathcal{U}$, where $\mathcal{U} = \{1, 4, 5, 20\}$, the set of all unitary divisors of 20.

*Theorem* 2.2 — If $N = \Pi p^{\alpha}$ and if

(1) $C$ is closed under the special operations;

(2) $e = \Pi p^{\epsilon}$ and $d = \Pi p^{\delta}$ are elements of $C$ such that for any $a = \Pi p^{\beta} \in C$, conditions (i) to (iii) of Theorem 2.1 hold, then $C$ is a Boolean ring with $e$ and $d$ as the identities under $\oplus$ and $\odot$ respectively.

PROOF: Using (ii) of Theorem 2.1, we note that

$$\text{(A)} \quad \begin{cases} p^{\beta_1} \oplus p^{\beta_2} = \begin{cases} p^{\epsilon}, \text{ if } \beta_1 = \beta_2 \\ p^{\alpha-\epsilon}, \text{ if } \beta_1 \neq \beta_2 \end{cases} \\ p^{\beta_1} \odot p^{\beta_2} = \begin{cases} p^{\beta_1}, \text{ if } \beta_1 \neq \beta_2 \\ p^{\epsilon}, \text{ if } \beta_1 \neq \beta_2. \end{cases} \end{cases}$$

Commutativity of $\oplus$ and $\odot$ follows from the definitions. In view of the fact that the gcd (lcm) of any two numbers is the product of the gcd's (lcm's) of the same prime powers that occur in the factorization of those two numbers, it is enough if we verify the Boolean ring conditions when $N = p^{\alpha}$, for a prime number $p$. This can be done using (A).

All the examples mentioned earlier illustrate Theorem 2.2.

*Note* : If the Boolean ring $C$ is $\mathcal{CV}$, then $e = 1$.

*Corollary* 2.2.1 — $\mathcal{U}$ is a Boolean ring with respect to $\oplus$ and $\odot$ with identities 1 and $N$ respectively.

Note (2) of Theorem 2.1 and Theorem 2.2 yield.

*Theorem* 2.3 — A necessary and sufficient condition for $C$ which is closed with respect to $\oplus$ and $\odot$ to form a Boolean ring with $e$ and $d$ as identities, respectively, are the conditions (i) to (iii) of Theorem 2.1.

*Remark* : For every '$a$' dividing $N$, there is a Boolean ring of divisors of $N$ containing '$a$'.

For,

$$\text{let } N = \Pi\, p_t^{\alpha_t} \quad \text{and} \quad a = \Pi\, p_t^{\beta_t},\ 0 \leqslant \beta_t \leqslant \alpha_t,\ \forall\ t.$$

We may write $a = \Pi\, p_i^{\beta_i}\ \Pi\, p_j^{\beta_j}$, where $\beta_i \leqslant \alpha_{i/2}$ and $\beta_j > \alpha_{j/2}$.

We now take $e = \Pi\, p_i^{\beta_i}\ \Pi\, p_j^{\alpha_j - \beta_j}$, so that for every $p_j$, $\epsilon_j = \alpha_j - \beta_j < \alpha_{j/2}$. Then $\{e, a\}$ is a Boolean ring with respect to $\oplus$ and $\odot$.

*Corollary* 2.3.1 — If $a^2 = N$, then the only Boolean ring of divisors of $N$ containing $a$ is the trivial one $\{a\}$.

*Corollary* 2.3.2 — If $e = \Pi\, p^{\epsilon}$ where $\epsilon$'s satisfy the condition (iii) of theorem 2.1, then there is a maximal Boolean ring (i.e. maximal set of divisors forming Boolean ring) $\mathcal{M}_{e,N}$ containing $e$ as additive identity, for which $N/e$ is the multiplicative identity.

PROOF : Consider the set

$$\mathcal{M}_{e,N} = (a : a = \prod_{p \mid N} p^{\beta},\ \beta = \epsilon \text{ or } \beta = \alpha - \epsilon\}.$$

where $N = \Pi\, p^{\alpha}$.

This can be seen to be a Boolean ring. If $\mathcal{M}$ is any other Boolean ring with $e$ as the additive identity, then $b = \Pi\, p^{\beta} \in \mathcal{M} \Rightarrow \beta = \epsilon$ or $\beta = \alpha - \epsilon$, for every prime $p \mid N \Rightarrow b \in \mathcal{M}_{e,N}$, which leads to the result.

## 3. BOOLEAN CONVOLUTION

An arithmetic function $f$ is one whose domain is the set of all positive integers and whose range is a subset of the complex number field (we can in fact take a sub-set of an arbitrary field as the range of $f$ but here we refrain from doing so).

$f$ is said to be multiplicative if $f(NN') = f(N)\, f(N')$, for $(N, N') = 1$.

Let $e$ be an arbitrary but fixed natural number. Throughout the ensuing discussion, we choose $e > 1$ unless specified otherwise.

Let us associate with every natural number $N$ a set $B_N$ defined by

$$B_N = \begin{cases} \mathcal{M}_{e,N}, \text{ if } e \mid N \text{ and the first part of (iii) of Theorem 2.1 holds,} \\ \phi \text{ (empty set), otherwise.} \end{cases} \qquad \ldots(3.1)$$

A Boolean convolution '*' of two arithmetic functions $f$ and $g$ is defined by

$$(f * g)(N) = \begin{cases} \Sigma f(d)\, g(N/d)\ (d \in \mathcal{M}_{e,N}), & \text{if } B_N = \mathcal{M}_{e,N} \\ 0 \quad , & \text{if } B_N = \phi. \end{cases} \qquad \ldots(3.2)$$

*Remark* : If $e = 1$, the Boolean convolution reduces to the so called unitary product [see for instance Cohen (1961)].

We now obtain some properties of the Boolean convolution, which we need for our subsequent work.

1. *The Boolean convolution is not associative* — For, consider the arithmetic functions $E$ and $I$ defined by

$$E(N) = 1, \text{ for all } N$$

$$I(N) = N, \text{ for all } N.$$

Choose $e = 6$, $N = 432$. Then, $\mathcal{M}_{e,N} = \{6, 18, 24, 72\}$. So that

$$((E * E) * I)(432) = 12, (E * (E * I))(432) = 18$$

2. *It is commutative* — For, suppose $B_N = \phi$. Then,

$$(f * g)(N) = (g * f)(N) = 0.$$

Again if $B_N = \mathcal{M}_{e,N}$, $d \in \mathcal{M}_{e,N} \Leftrightarrow N/d \in \mathcal{M}_{e,N}$, so that

$$(f * g)(N) = \Sigma f(d)\, g(N/d)\ (d \in \mathcal{M}_{e,N})$$

$$= \Sigma\, g(\delta) f(N/\delta) \quad (\delta \in \mathcal{M}_{e,N})$$

$$= (g * f)(N)$$

3. *No arithmetic function can be an identity for the Boolean convolution* — For, choose $N = e$, so that $B_N = \phi$.

Suppose $\eta$ is an identity. Then,

$$(I * \eta)(e) = 0,\ I(e) = e.$$

Therefore,

$$I * \eta \neq I, \text{ a contradiction.}$$

We now state the following:

*Theorem* 3.1 — Let $\mathcal{T}$ be the set of all arithmetic functions. Then $\mathcal{T}$, with pointwise addition '+' defined by $(f + g)(N) = f(N) + g(N)$ and the Boolean convolution '*' is a non-associative but commutative ring, without identity, except in the case when $e = 1$.

PROOF : In view of what we proved earlier, only the last part of the theorem needs a proof. Indeed when $e = 1$, the unitary product is not only associative but even the identity exists, which can be verified to be

$$\delta(N) = \begin{cases} 1, & \text{if } N = 1, \\ 0, & \text{otherwise.} \end{cases}$$

*Zero Divisors in* $\mathcal{T}$

It is curious to note that every arithmetic function is a zero divisor.

For, let $g$ be an arithmetic function. Then,

$$(\lambda * g)(N) = 0, \ \forall\ N,$$

where $$\lambda(N) = \begin{cases} 0, & \text{if } e \mid N, \\ 1, & \text{otherwise.} \end{cases}$$

*A Multiplicative Property*

We observe that the Boolean convolution of two multiplicative arithmetic functions is not multiplicative.

For example, let $e = 6$, $N = 4$, $N' = 9$. Then $\mathcal{M}_{6,36} = \{6\}$,

$\mathcal{M}_{6,4} = \phi$, $\mathcal{M}_{6,9} = \phi$. So that,

$(I * E)(36) = 6$, $(I * E)(4) = 0$, $(I * E)(9) = 0$.

Therefore,

$$(I * E)(36) \neq (I * E)(4)\,(I * E)(9).$$

However, we notice the following special type of multiplicative property. When $B_N = \mathcal{M}_{e,N}$, let us write

$$F_e(N) = \Sigma f(d)\, g(N/d) \ (d \in \mathcal{M}_{e,N})$$

*Theorem* 3.2 — Let $f, g$ be two multiplicative arithmetic functions, and let $(N, N') = 1$. Then,

(i) $(f * g)(NN') = (f * g)(N)\,(f * g)(N')$, if $B_{NN'} = \phi$,

(ii) $F_e(NN') = F_{e_1}(N)\, F_{e_2}(N')$, if $B_{NN'} = \mathcal{M}_{e,NN'}$,

where $e_1 = (e, N)$, $e_2 = (e, N')$.

PROOF : (i) can be seen from

$$B_{NN'} = \phi \Rightarrow B_N = \phi \text{ or } B_{N'} = \phi.$$

(ii) is evident from the fact that $f$ and $g$ are multiplicative and $\mathcal{M}_{e,NN'} = \mathcal{M}_{e_1,N} \times \mathcal{M}_{e_2,N'}$, where $\mathcal{M}_{e_1,N} \times \mathcal{M}_{e_2,N'} = \{d_1 d_2 : d_1 \in \mathcal{M}_{e_1,N}, d_2 \in \mathcal{M}_{e_2,N'}\}$.

ACKNOWLEDGEMENT

The author is indebted to Prof. K. Sitaram, Dr V. V. S. Sastri and the referee for their valuable suggestions in the preparation of the paper.

REFERENCES

Cohen, Eckford (1961). Unitary products of arithmetic functions, *Acta Arith.*, **7**, 29–38.

Halmos, Paul R. (1967). Lectures on Boolean Algebras. D. Van Nostrand Company, Inc., New York.