ON THE THEORY OF RING-LOGICS

ADIL YAQUB

Introduction. Boolean rings $(B, \times, +)$ and Boolean logics (=Boolean algebras) $(B, \cap, *)$ are equationally interdefinable in a familiar way **(6)**. Foster's theory of ring-logics **(1; 2; 3)** raises this interdefinability and indeed the entire Boolean theory to a more general level. In this theory a ring (or an algebra) R is studied modulo K, where K is an arbitrary transformation group (or "Coordinate transformations") in R. The Boolean theory results from the special choice, for K, of the "Boolean group," generated by $x^* = 1 - x$ (order 2, $x^{**} = x$). More generally, in a commutative ring $(R, \times, +)$ with identity the *natural group* N, generated by $x^\wedge = 1 + x$ (with $x^\vee = x - 1$ as inverse) was shown to be of particular interest. Thus specialized to N, a commutative ring with identity $(R, \times, +)$ is called a *ring-logic*, mod N, if (1) the $+$ of the ring is equationally definable in terms of its N-logic $(R, \times, {}^\wedge, {}^\vee)$, and (2) the $+$ of the ring is *fixed* by its N-logic. It was shown **(2)** that each p-ring **(5)** is a ring-logic mod N. It was further shown **(3)** that each p^k-ring **(3; 5)** is a ring-logic mod D, where D is a somewhat more involved group.

All these known examples of ring-logics have zero radical, and the question presents itself: do there exist examples of ring-logics (modulo a suitable group) with non-zero radical? We shall answer this in the affirmative. Indeed, we shall show that the ring of residues mod n (n arbitrary) is a ring-logic modulo the natural group N itself.

1. The ring of residues mod p^k. Let $(R, \times, +)$ be a commutative ring with identity 1. We denote the generator of the natural group N by

(1.1) $$x^\wedge = 1 + x,$$

with inverse

(1.2) $$x^\vee = x - 1.$$

As in **(1)**, we define

(1.3) $$a \times_\wedge b = (a^\wedge \times b^\wedge)^\vee.$$

It is readily verified that

(1.4) $$a \times_\wedge b = a + b + ab.$$

The following notation is used **(2)**:

$$x^{\wedge n} = (\ldots((x^\wedge)^\wedge)\ldots)^\wedge; \quad x^{\vee n} = (\ldots((x^\vee)^\vee)\ldots)^\vee,$$

n iterations. Again

$$x^{\wedge kn} = (x^{\wedge k})^n; \quad x^{\vee kn} = (x^{\vee k})^n.$$

Received September 9, 1955.

https://doi.org/10.4153/CJM-1956-036-6 Published online by Cambridge University Press

We now consider $(R_{p^k}, \times, +)$, the ring of residues mod p^k (p prime) and prove the following

THEOREM 1. *$(R_{p^k}, \times, +)$ is a ring-logic* (mod N). *The ring $+$ is given by the following N-logical formula*

$$(1.5)\qquad x + y = \{(x(yx^{p^k-p^{k-1}-1})^{\wedge})x^{p^k-p^{k-1}}\}\times_{\wedge}$$
$$\{(x^{\wedge}(y(x^{\wedge})^{p^k-p^{k-1}-1})^{\wedge})^{\vee}(x^{p^k-p^{k-1}})^{\vee 2}\}.$$

Proof. By Euler's generalized form of Fermat's Theorem, we have

$$(1.6)\qquad a^{p^k-p^{k-1}} = 1,\ a \in R_{p^k},$$

a not divisible by p. We now distinguish two cases:

Case 1: Suppose p does not divide x. Then, by (1.6), the right side of (1.5) reduces to

$$\{x(1 + yx^{p^k-p^{k-1}-1})\cdot 1\}\times_{\wedge} 0 = x + yx^{p^k-p^{k-1}} = x + y,$$

since

$$(x^{p^k-p^{k-1}})^{\vee 2} = 1^{\vee 2} = 0;\ a \times_{\wedge} 0 = a.$$

This proves (1.5).

Case 2: Suppose p divides x. Then, clearly, p does not divide $x^{\wedge} = 1 + x$. Hence, using Case 1, the right side of (1.5) reduces to

$$0 \times_{\wedge}\{(x^{\wedge}(1 + y(x^{\wedge})^{p^k-p^{k-1}-1}))^{\vee}\cdot 1\} = (x^{\wedge} + y(x^{\wedge})^{p^k-p^{k-1}})^{\vee}$$
$$= (x^{\wedge} + y)^{\vee} = x + y,$$

since

$$(x^{p^k-p^{k-1}})^{\vee 2} = 0^{\vee 2} = 1;\ 0 \times_{\wedge} a = a.$$

Again (1.5) is verified. Hence $(R_{p^k}, \times, +)$ is *equationally* definable in terms of its N-logic. Next, we show that $(R_{p^k}, \times, +)$ is *fixed* by its N-logic.[1] Suppose then that there exists another ring $(R_{p^k}, \times, +')$, with the same class of elements R_{p^k} and the same $\times$ as $(R_{p^k}, \times, +)$ and which has the *same logic* as $(R_{p^k}, \times, +)$. To prove that $+ = +'$. Again we distinguish two cases.

Case 1: p does not divide x. Then

$$x +' y = x(1 +' yx^{p^k-p^{k-1}-1}) = x(yx^{p^k-p^{k-1}-1})^{\wedge} = x(1 + yx^{p^k-p^{k-1}-1}) = x + y,$$

since, by hypothesis, $x^{\wedge} = 1 + x = 1 +' x$.

[1]A ring $(R, \times, +)$ is said to be fixed by its N-logic if there exists no other ring $(R, \times, +')$, on the same set R and with the same $\times$ but with $+' \neq +$, which has the same N-logic; i.e.,

$$x^{\wedge} = 1 + x = 1 +' x;\ x^{\vee} = x - 1 = x -' 1.$$

https://doi.org/10.4153/CJM-1956-036-6 Published online by Cambridge University Press

Case 2: p divides x. Then, clearly, p does not divide $x^{\wedge} = 1 + x$. Hence, by Case 1,

$$x +' y = x^{\wedge} +' y^{\vee} = x^{\wedge} + y^{\vee} = x + y.$$

Therefore $+' = +$, and the theorem is proved.

COROLLARY. $(R_p, \times, +) = (F_p, \times, +)$, *the ring (field) of residues* (mod p), *p prime, is a ring-logic* (mod N) *the $+$ being given by setting $k = 1$ in* (1.5), *and making use of $x^p = x$:*

$$(1.7)^2 \qquad x + y = \{(x(x^{p-2}y)^{\wedge})\} \times_{\wedge} \{(x^{\wedge}((x^{\wedge})^{p-2}y)^{\wedge})^{\vee}(x^{p-1})^{\vee 2}\}.$$

2. The ring of residues (mod n), n arbitrary. In attempting to generalize Theorem 1 to the residue class ring $(R_n, \times, +)$, where n is *any* positive integer, the following concept of independence, introduced by Foster **(4)**, is needed.

Definition. Let $\tilde{\mathfrak{A}} = \{\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n\}$ be a finite set of algebras of the same species $\mathfrak{S}$. We say that the algebras $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$ are *independent* if, corresponding to each set $\{\phi_i\}$ of expressions of species $\mathfrak{S}$ $(i = 1, \ldots, n)$, there exists at least one expression X such that

$$\phi_i = X \pmod{\mathfrak{A}_i} \qquad (i = 1, \ldots, n).$$

By an *expression* we mean some composition of one or more indeterminate-symbols $\zeta, \ldots$ in terms of the primitive operations of $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$; $\phi = X$ (mod $\mathfrak{A}$), also written as $\phi = X(\mathfrak{A})$, means that this is an identity of the algebra $\mathfrak{A}$.

We now prove the following

THEOREM 2. *Let* $(\mathfrak{A}_1, \times, +), \ldots, (\mathfrak{A}_t, \times, +)$ *be a finite set of ring-logics* (mod N), *such that the N-logics* $(\mathfrak{A}_1, \times, {}^{\wedge}), \ldots, (\mathfrak{A}_t, \times, {}^{\wedge})$ *are independent. Then* $\mathfrak{A} = \mathfrak{A}_1 \times \ldots \times \mathfrak{A}_t$ *(direct product) is also a ring-logic* (mod N).

Proof. Since $\mathfrak{A}_i$ is a ring-logic (mod N), there exists an N-logical expression ϕ_i such that, for every $x_i, y_i \in \mathfrak{A}_i$ $(i = 1, \ldots, t)$,

$$x_i + y_i = \phi_i = \phi_i(x_i, y_i;\ \times, {}^{\wedge}, {}^{\vee}) = \phi_i(x_i, y_i;\ \times, {}^{\wedge}).$$

In view of the independence of the logics, there exists an expression X such that

$$X = \begin{cases} \phi_1 \pmod{\mathfrak{A}_1}, \\ \ldots \\ \phi_t \pmod{\mathfrak{A}_t}. \end{cases}$$

Then, for $a = (a_1, a_2, \ldots, a_t) \in \mathfrak{A}$; $b = (b_1, b_2, \ldots, b_t) \in \mathfrak{A}$, we have

[2]This formula is considerably shorter than the formulas for $+$ given in **(2; 3)**.

https://doi.org/10.4153/CJM-1956-036-6 Published online by Cambridge University Press

$$\begin{aligned} X(a, b; \times, {}^\wedge) &= X((a_1, a_2, \ldots, a_t), (b_1, b_2, \ldots, b_t); \times, {}^\wedge) \\ &= (X(a_1, b_1; \times, {}^\wedge), X(a_2, b_2; \times, {}^\wedge), \ldots, X(a_t, b_t; \times, {}^\wedge)) \\ &= (a_1 + b_1, a_2 + b_2, \ldots, a_t + b_t) \\ &= (a_1, a_2, \ldots, a_t) + (b_1, b_2, \ldots, b_t) \\ &= a + b; \end{aligned}$$

i.e.,

$$a + b = X(a, b; \times, {}^\wedge); a, b \in \mathfrak{A}.$$

Hence, $\mathfrak{A} = \mathfrak{A}_1 \times \ldots \times \mathfrak{A}_t$ is *equationally* definable in terms of its N-logic. Next, we show that $\mathfrak{A}$ is fixed by its N-logic. Suppose there exists a $+'$ such that $(\mathfrak{A}, \times, +')$ is a ring, with the same class of elements $\mathfrak{A}$ and the same $\times$ as the ring $(\mathfrak{A}, \times, +)$, and which has the *same logic* $(\mathfrak{A}, \times, {}^\wedge)$ as the ring $(\mathfrak{A}, \times, +)$. To prove that $+ = +'$.

Now, let $a = (a_1, a_2, \ldots, a_t) \in \mathfrak{A}$; $b = (b_1, b_2, \ldots, b_t) \in \mathfrak{A}$. A new $+'$ in $\mathfrak{A}$ defines and is defined by new $+'_1$ in $\mathfrak{A}_1$, $+'_2$ in $\mathfrak{A}_2, \ldots, +'_t$ in $\mathfrak{A}_t$, such that $(\mathfrak{A}_1, \times, +'_1)$ is a ring, and similarly for $(\mathfrak{A}_2, \times, +'_2), \ldots, (\mathfrak{A}_t, \times, +'_t)$; i.e.,

$$\begin{aligned} a +' b &= (a_1, a_2, \ldots, a_t) +' (b_1, b_2, \ldots, b_t) \\ &= (a_1 +'_1 b_1, a_2 +'_2 b_2, \ldots, a_t +'_t b_t). \end{aligned} \tag{2.1}$$

Furthermore, the assumption that $(\mathfrak{A}, \times, +')$ has the same logic as $(\mathfrak{A}, \times, +)$ is equivalent to the assumption that $(\mathfrak{A}_1, \times, +'_1)$ has the same logic as $(\mathfrak{A}_1, \times, +)$, and similarly for $(\mathfrak{A}_i, \times, +'_i)$ and $(\mathfrak{A}_i, \times, +)(i = 2, \ldots, t)$. Since $(\mathfrak{A}_1, \times, +)$ is a ring-logic, and hence with its $+$ fixed, it follows that $+'_1 = +$; similarly $+'_2 = +, \ldots, +'_t = +$. Hence, using (2.1), $+' = +$, and the proof is complete.

We shall now prove the following

LEMMA 3. *Let $p_1, \ldots, p_t$ be distinct primes, and let*

$$(R_{n_i}, \times, +), \; n_i = p_i^{k_i} = p_i m_i; \; i = 1, \ldots, t,$$

be a set of residue class rings (mod n_i). *Then the logics* $(R_{n_i}, \times, {}^\wedge)(i = 1, \ldots, t)$ *are independent.*

Proof. Let

$$P(i) = \prod_{j=1}^{t} n_j, \qquad j \neq i,$$

Then, clearly

$$(P(i), n_i) = 1.$$

Hence, there exist integers $r_i > 0$, $s_i > 0$ such that

$$r_i P(i) - s_i n_i = 1.$$

Now, define

$$\epsilon(x) = x^{(n_1 - m_1)(n_2 - m_2)\ldots(n_t - m_t)}.$$

https://doi.org/10.4153/CJM-1956-036-6 Published online by Cambridge University Press

Then one easily verifies that, for $i \neq j$,

$$\omega_i = \omega_i(x) = \{\epsilon(x) \times_\Lambda ((\epsilon(x))^{\vee})^{(n_1 - m_1)\ldots(n_t - m_t)}\}^{\Lambda r_i P(i) - 1} = \begin{cases} 1 (R_{n_i}) \\ 0 (R_{n_j}) \end{cases}.$$

Now, to prove the independence of the logics $(R_{n_i}, \times, {}^\Lambda)$, let $\{\phi_i\}$ be a set of t expressions of species $\times, {}^\Lambda$; i.e., a primitive composition of indeterminate-symbols in terms of the operations $\times, {}^\Lambda$; then, if we define (cf. **4**)

$$X = \phi_1\omega_1 \times_\Lambda \phi_2\omega_2 \times_\Lambda \ldots \times_\Lambda \phi_t\omega_t,$$

we immediately obtain

$$\phi_i = X (\text{mod } R_{n_i}),$$

since $a \times_\Lambda 0 = a = 0 \times_\Lambda a$. This proves the theorem.

Recalling the well-known fact that

$$(R_n, \times, +) \cong R_{n_1} \times \ldots \times R_{n_t} \text{ (direct product)}, \tag{2.2}$$

n arbitrary, $n = n_1 \ldots n_t$, a combination of Theorems 1, 2, Lemma 3 and (2.2) readily yields

THEOREM 4 (Fundamental Theorem on R_n as ring-logics). $(R_n, \times, +)$, *the residue class ring* (mod n), *n arbitrary, is a ring-logic* (mod N).

We conclude with several illustrative examples.

Example 1. $R_{p^k} = R_2 = F_2 = \{0, 1\}$.
It is readily verified that each of (1.5) and (1.7) reduces to the familiar Boolean formula

$$x + y = xy^\Lambda \times_\Lambda x^\Lambda y. \tag{2.3}$$

Example 2. $R_{p^k} = R_3 = F_3 = \{0, 1, 2\}$.
Formula (1.7) yields

$$x + y = \{x(xy)^\Lambda\} \times_\Lambda \{[(x^\Lambda (x^\Lambda y)^\Lambda)]^\vee (x^2)^{\vee 2}\}. \tag{2.4}$$

Compare with **(1)** in which the following formula was obtained:

$$x + y = xy^\Lambda \times_\Lambda x^\Lambda y \times_\Lambda x^2 y^2. \tag{2.5}$$

It is noteworthy to observe that the $+$ of $(F_p, \times, +)$, the field of residues (mod p), p prime, may also be expressed in the following form:

$$x + y = \{x(yx^{p-2})^\Lambda\} \times_\Lambda \{y(x^\Lambda x^{\Lambda 2} \ldots x^{\Lambda p-1})^2\}. \tag{2.6}$$

or by

$$x + y = \{x(yx^{p-2})^\Lambda\} \times_\Lambda \{y(x^{p-1})^{\vee 2}\}. \tag{2.7}$$

The last formula, when specialized to F_3, gives a simpler expression for $+$ than (2.4).

https://doi.org/10.4153/CJM-1956-036-6 Published online by Cambridge University Press

Example 3. $R_{pk} = R_{22} = \{0, 1, 2, 3\}$.
Formula (1.5) reduces to

$$(2.8) \qquad x + y = \{(x(xy)^{\wedge}x^2)\} \times_{\wedge} \{[(x^{\wedge}(x^{\wedge}y)^{\wedge})]^{\vee}(x^2)^{\vee 2}\}.$$

It may be verified that the $+$ in $(R_4, \times, +)$ is also given by

$$(2.9) \qquad x + y = \{(xy)^{\wedge}(xy)^2 \times_{\wedge} (x \times_{\wedge} y)(xy)^{\wedge 2}\}\{(xy)(xy)^{2\vee}\}^{\wedge}.$$

This last formula excels most of the others in obviously displaying the symmetry of $+$.

Example 4. $R_n = R_6 = \{0, 1, 2, 3, 4, 5\}$.
The correspondence

$$\begin{array}{ll} 0 \leftrightarrow (0_2, 0_3), & 3 \leftrightarrow (1_2, 0_3), \\ 1 \leftrightarrow (1_2, 1_3), & 4 \leftrightarrow (0_2, 1_3), \\ 2 \leftrightarrow (0_2, 2_3), & 5 \leftrightarrow (1_2, 2_3), \end{array}$$

determines an isomorphism of R_6 and $R_2 \times R_3$ (direct product), where $R_2 = \{0_2, 1_2\}$ and $R_3 = \{0_3, 1_3, 2_3\}$.

It is readily verified (compare with the proof of Lemma 3 and (2.3), (2.5) above) that

$$(2.10) \quad x + y = \{(xy^{\wedge} \times_{\wedge} x^{\wedge}y)(x^2 \times_{\wedge} (x^2)^{\vee 2})^{\wedge 2}\}$$
$$\times_{\wedge} \{(xy^{\wedge} \times_{\wedge} x^{\wedge}y \times_{\wedge} x^2y^2)(x^2 \times_{\wedge} (x^2)^{\vee 2})^{\wedge 3}\}.$$

Formula (2.10) may be verified either by direct substitution from R_6, or via the $R_2 \times R_3$ representation above.

References

1. A. L. Foster, *On n-ality theories in rings and their logical algebras, including tri-ality principle in three-valued logics*, Amer. J. Math., *72* (1950), 101–123.
2. ———, *p-rings and ring-logics*, Univ. Calif. Publ., *1* (1951), 385–396.
3. ———, *p^k-rings and ring-logics*, Ann. Scu. Norm. Pisa, *5* (1951), 279–300.
4. ———, *Unique subdirect factorization within certain classes of universal algebras*, Math. Z., *62* (1955), 171–188.
5. N. H. McCoy and D. Montgomery, *A representation of generalized Boolean rings*, Duke Math. J., *3* (1937), 455–459.
6. M. H. Stone, *The theory of representations of Boolean algebras*, Trans. Amer. Math. Soc., *40* (1936), 37–111.

University of California, Berkeley
and
Purdue University

https://doi.org/10.4153/CJM-1956-036-6 Published online by Cambridge University Press