ON CERTAIN FINITE RINGS AND RING-LOGICS

ADIL YAQUB

Introduction. Boolean rings $(B, \times, +)$ and Boolean logics (=Boolean algebras) $(B, \cap, {}^*)$ though historically and conceptionally different, are equationally interdefinable in a familiar way [6]. With this equational interdefinability as motivation, Foster introduced and studied the theory of ring-logics. In this theory, a ring (or an algebra) R is studied modulo K, where K is an arbitrary transformation group 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 1, the *natural group* N, generated by $x^{\wedge} = 1 + x$ (with $x^{\vee} = x - 1$ as inverse) proved 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. Several classes of ring-logics (modulo suitably chosen groups) are known [1; 2; 7], and the object of this manuscript is to extend further the class of ring-logics. Indeed, we shall prove the following:

THEOREM 1. *Let R be any finite commutative ring with zero radical. Then, R is a ring-logic, mod N.*

1. The finite field case. Let $(R, \times, +)$ be a commutative ring with identity 1. We denote the generator of the natural group by $x^{\wedge} = 1 + x$, with inverse $x^{\vee} = x - 1$. Following [1], we define $a \times_{\wedge} b = (a^{\wedge} \times b^{\wedge})^{\vee}$. It is readily verified that $a x_{\wedge} b = a + b + ab$.

Let $(F_{p^k}, \times, +)$ be a finite field with exactly p^k elements (p prime). We now have the following:

THEOREM 2. *$(F_p k, \times, +)$ is a ring logic (mod N). Indeed, the ring (field) $+$ is given by the following N-logical formula:*

$$x + y = \{(x(yx^{p^k-2})^{\wedge})\} \times_{\wedge} \{y((x^{p^k-1})^{\vee})^2\} . \tag{1.1}$$

Proof. It is well known that in the Galois field F_{p^k}, we have

$$a^{p^k-1} = 1, a \in F_{p^k}, a \neq 0 . \tag{1.2}$$

we now distinguish two cases:

Received August 29, 1961.

Case 1. Suppose $x \neq 0$. Then, by (1.2), the right-side of (1.1) reduces to $\{x(1 + yx^{p^k-2})\} \times_{\wedge} 0 = x + yx^{p^k-1} = x + y$, since $((x^{p^k-1})^{\vee})^2 = (1^{\vee})^2 = 0$; $a \times_{\wedge} 0 = a$. This proves (1.1).

Case 2. Suppose $x = 0$. Then, $x^{\wedge} = 1 + x = 1$. Hence, the right side of (1.1) reduces to $0 \times_{\wedge} \{y((0^{\vee})^2\} = y = 0 + y = x + y$, since $((x^{p^k-1})^{\vee})^2 = (0^{\vee})^2 = 1$; $0 \times_{\wedge} a = a$. Again, (1.1) is verified. Hence, $(F_{p^k}, \times, +)$ is *equationally* definable in terms of its N-logic. Next, we show that $(F_pk, \times, +)$ is *fixed* by its N-logic. Suppose then that there exists another ring $(F_pk, \times, +')$, with the same class of elements F_pk and the same "$\times$" as $(F_pk, \times, +)$ and which has the *same logic* as $(F_pk, \times, +)$. To prove that $+' = +$. Again, we distinguish two cases.

Case 1. Suppose $x \neq 0$. Then, using (1.2), we have $x +' y = x(1 +' yx^{p^k-2}) = x(yx^{p^k-2})^{\wedge} = x(1 + yx^{p^k-2}) = x + y$, since, by hypothesis, $x^{\wedge} = 1 + x = 1 +' x$.

Case 2. Suppose $x = 0$. Then, $x +' y = 0 +' y = y = 0 + y = x + y$. Therefore, $+' = +$, and the theorem is proved.

COROLLARY. *$(F_p, \times, +)$, the ring (field) of residues* (mod p), *p prime, is a ring-logic* (mod N) *the $+$ being given by setting $k = 1$ in* (1.1):

$$x + y = \{(x(yx^{p-2})^{\wedge})\} \times_{\wedge} \{y((x^{p-1})^{\vee})^2\} . \tag{1.3}$$

2. The general case. In attempting to extend Theorem 2 to *any* finite commutative ring with zero radical, the following concept of independence, introduced by Foster [3], is needed.

DEFINITION. Let $\bar{A} = \{A_1, A_2, \cdots, A_n\}$ be a finite set of algebras of the same species Sp. We say that the algebras $A_1, A_2, \cdots, A_n$ satisfy the *Chinese residue condition*, or are *independent*, if, corresponding to each set $\{\varphi_i\}$ of expressions of species Sp $(i = 1, \cdots, n)$, there exists at least on expression Ψ such that $\Psi = \varphi_i \pmod{A_i}$ $(i = 1, \cdots, n)$. By an *expression* we mean some composition of one or more indeterminate-symbols $\xi, \cdots$, in terms of the primitive operations of $A_1, A_2, \cdots, A_n$; $\Psi = \varphi \pmod{A}$, also written $\Psi = \varphi(A)$, means that this is an identity of the Algebra A.

We shall now extend the concept of ring-logic to the direct sum of certain ring-logics. We shall denote the direct sum of the rings A_1 and A_2 by $A_1 \oplus A_2$. The direct power A^m will denote $A \oplus A \oplus \cdots \oplus A$ (m summands).

THEOREM 3. *Let* $(A_1, \times, +), \cdots, (A_t, \times, +)$ *be a finite set of ring-logics* (mod N), *and let the N-logics* $(A_1, \times, \hat{}, \check{}), \cdots, (A_t, \times, \hat{}, \check{})$ *be independent. Then* $A = A_1^{m_1} \oplus \cdots \oplus A_t^{m_t}$ *is also a ring-logic* (mod N).

Proof. Since A_i is a ring-logic (mod N), there exist an N-logical expression φ_i such that, for every $x_i, y_i \in A_i$ $(i = 1, \cdots, t)$,

$$x_i + y_i = \varphi_i = \varphi_i(x_i, y_i; \times, \hat{}, \check{}) .$$

Since the N-logics are independent, there exists an expression X such that

$$X = \begin{cases} \varphi_1(\text{mod } A_1) \\ \cdots \\ \varphi_t(\text{mod } A_t) . \end{cases}$$

Therefore, for every $x_i, y_i \in A_i$ $(i = 1, \cdots, t)$,

$$x_i + y_i = \varphi_i = X = X(x_i, y_i; \times, \hat{}, \check{},) .$$

Hence, the N-logical expression X represents the $+$ of *each* A_i. Since "$+$" and "$\times$" are component-wise in A, therefore, for all $x, y \in A$,

$$x + y = X(x, y; \times, \hat{}, \check{}).$$

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

Now, let $a = (a_{11}, \cdots, a_{1m_1}, a_{21}, \cdots, a_{2m_2}, \cdots, a_{t1}, \cdots, a_{tm_t}) \in A$. A new $+'$ in A defines and is defined by new $+_1'$ in A_1, $+_2'$, in $A_2, \cdots$, $+_t'$ in A_t, such that $(A_i, \times, +_i')$ is a ring $(i = 1, \cdots, t)$; i.e., for $a, b \in A$,

$$\begin{aligned} (2.1) \qquad a +' b &= (a_{11}, \cdots, a_{21}, \cdots, a_{t1}, \cdots) +' (b_{11}, \cdots, b_{21}, \cdots, b_{t1}, \cdots) \\ &= (a_{11} +_1' b_{11}, \cdots, a_{21} +_2' b_{21}, \cdots, a_{t1} +_t' b_{t1}, \cdots) . \end{aligned}$$

Furthermore, the assumption that $(A, \times, +')$ has the same logic as $(A, \times, +)$ is equivalent to the assumption that $(A_1, \times, +_1')$ has the same logic as $(A_1, \times, +)$, and similarly for $(A_i, \times, +_i')$ and $(A_i, \times, +)$ $(i = 2, \cdots, t)$. Since $(A_1, , \times +)$ is a ring-logic, and hence with its $+$ fixed, it follows that $+_1' = +$; similarly $+_2' = +, \cdots, +_t' = +$. Hence, using (2.1), $+' = +$, and the proof is complete.

A careful examination of the proof of Theorem 3 shows that the independence of the logics was *not* used in the "fixed" part of the proof. Hence, we have the following

COROLLARY. *Let* $(A_1, \times, +), \cdots, (A_t, \times, +)$ *be a finite set of ring-*

logics (mod N). *Then,* $A_1^{m_1} \oplus \cdots \oplus A_t^{m_t}$ *is fixed by its N-logic.*

We now examine the independence of the logics $(F_{p_i}^{m_i}k_i, \times, +)$ $(i = 1, \cdots, t)$.

THEOREM 4. *Let* $p_1, \cdots, p_t$ *be distinct primes, and let* $F_{p_i}^{m_i}k_i$ *be the* m_i *direct power of the Galois field* $F_{p_i}k_i$ $(i = 1, \cdots, t)$. *Then the logics* $(F_{p_i}^{m_i}k_i, \times, \hat{}, \check{})$ $(i = 1, \cdots, t)$ *are independent.*

Proof. Let $n_i = p_i^{k_i}$, and let $P(i) = \prod_{j=1}^{t} n_j, j \neq i$. Let $F_i = F_{p_i}k_i$ $(i = 1, \cdots, t)$. Clearly, $P(i)$ and n_i are relatively prime. Hence, there exist integers $r_i > 0, s_i > 0$ such that $r_i P(i) - s_i n_i = 1$. Define $\varepsilon(x)$ and $\delta(x)$ as follows:

$$\varepsilon(x) = x^{(n_1-1)(n_2-1)\cdots(n_t-1)};\ \delta(x) = \varepsilon(x) \times_{\wedge} ((\varepsilon(x))^{\vee})^2 .$$

It is easily seen that $\delta(x) = 1, x \in F_i^{m_i}$ $(i = 1, \cdots, t)$. Let $x^{\wedge k} = (\cdots((x^{\wedge})^{\wedge})^{\wedge}\cdots)^{\wedge}$, k iterations. Then one easily verifies that for $i \neq j$,

$$w_i = w_i(x) = (\delta(x))^{\wedge s_i n_i} = \begin{cases} 1 \pmod{F_i^{m_i}} \\ 0 \pmod{F_j^{m_j}} \end{cases} .$$

Now, to prove the independence of the logics $(F_i^{m_i}, \times, \hat{}, \check{})$ $(i = 1, \cdots, t)$, let $\{\delta_i'\}$ be any set of t expressions of species $\times, \hat{}, \check{}$; i.e., a primitive composition of indeterminate-symbols in terms of the operations $\times, \hat{}, \check{}$. Let $X = \delta_1' w_1 \times_{\wedge} \delta_2' w_2 \times_{\wedge} \cdots \times_{\wedge} \delta_t' w_t$. Then it is easily seen that $X = \delta_i' \pmod{F^{im_i}}$ $(i = 1, \cdots, t)$, since $a \times_{\wedge} 0 = a = 0 \times_{\wedge} a$, and the theorem is proved.

We are now in a position to prove the following theorem (see introduction).

THEOREM 5. *Any finite commutative ring R with zero radical is a ring-logic* (mod N).

Proof. First, if R consists of one element, then $R = \{0\}$. Clearly, R is a ring-logic (mod N) in this case, since $a + b = a \times b$, for example. Hence, assume that R has more than one element. It is well known (see [5]) that any finite commutative ring R with zero radical and with more than one element is isomorphic to the complete direct sum of a finite number of finite fields $F_{p_1}k_1, \cdots, F_{p_t}k_t$: i.e., $R \cong F_{p_1}k_1 \oplus \cdots \oplus F_{p_t}k_t$. Now, by Theorem 2, *each* $(F_{p_i}k_i, \times, +)$ is a ring-logic (mod N). Hence, by the corollary to Theorem 3, $F_{p_1}k_1 \oplus \cdots \oplus F_{p_t}k_t$ is *fixed* by its N-logic. Therefore, by the above isomorphism, R, too, is fixed by its N-logic, and there only remains to show that the $+$ of R is *equationally* definable in terms of its N-logic. To this end, we distinguish two cases.

Case 1. Suppose $p_1, \cdots, p_t$ are all *distinct*. By Theorem 2, $(F_{p_i}k_i, \times, +)$ is a ring-logic (mod N) $(i = 1, \cdots, t)$. By Theorem 4 (with $m_1 = \cdots = m_t = 1$), the N-logics $(F_{p_i}k_i, \times, \hat{}, \check{})$ are independent $(i = 1, \cdots, t)$. Therefore, by Theorem 3 (with $m_1 = \cdots = m_t = 1$), the direct sum $F_{p_1}k_1 \oplus \cdots \oplus F_{p_t}k_t$ (and hence R, by the above isomorphism) is a ring-logic (mod N). Hence, in particular, the $+$ of R is equationally definable in terms of its N-logic.

Case 2. Suppose $p_1, \cdots, p_t$ are *not* all distinct. Let $q_1, \cdots, q_r$ be the *distinct* primes in $\{p_1, \cdots, p_t\}$. Since the Galois fields F_pk_i and F_pk_j are both subfields of $F_pk_ik_j$, it is easily seen that $F_{p_1}k_1 \oplus \cdots \oplus F_{p_t}k_t$ is a *subring* of a direct sum of direct powers of $F_{q_i}h_i$ $(i = 1, \cdots, r)$; i.e., $F_{p_1}k_1 \oplus \cdots \oplus F_{p_t}k_t$ is a subring of $F_{q_1}^{m_1}h_1 \oplus \cdots \oplus F_{q_r}^{m_r}h_r$, for some positive integers $h_1, \cdots, h_r, m_1, \cdots, m_r$. Now, the rest of the proof is similar to that of *Case* 1. Thus, by Theorem 2, $(F_{q_i}h_i, \times, +)$ is a ring-logic (mod N) $(i = 1, \cdots, r)$. By Theorem 4, the N-logics $(F_{q_i}h_i, \times, \hat{}, \check{})$ are idependent $(i = 1, \cdots, r)$. Hence, by Theorem 3, $F_{q_1}^{m_1}h_1 \oplus \cdots \oplus F_{q_r}^{m_r}h_r$ is a ring-logic (mod N). Therefore, in particular, the $+$ of $F_{q_1}^{m_1}h_1 \oplus \cdots \oplus F_{q_r}^{m_r}h_r$ is equationally definable in terms of its N-logic. Hence, afortiori, the $+$ of the *subring* $F_{p_1}k_1 \oplus \cdots \oplus F_{p_t}k_t$ (and therefore the $+$ of R, by the above isomorphism) is equationally definable in terms of the N-logic of R. Therefore, R is a ring-logic (mod N), and the theorem is proved.

3. **p-rings and p^k-rings.** We shall now make an attempt to generalize Theorem 3, and apply this generalization to p-rings and p^k-rings. We first observe that the proof of Theorem 3 does *not* depend on the cardinality of the powers m_i. Furthermore, the proof still remains valid if one considers a *subdirect* sum of *subdirect* powers of A_i instead of the *complete* direct sum of direct powers of A_i $(i = 1, \cdots, t)$. In view of this, Theorem 3 can now be cast in the following more general form.

THEOREM 3′. *Let $(A_1, \times, +), \cdots, (A_t, \times, +)$ be a finite set of ring-logics* (mod N), *and let the N-logics $(A_1, \times, \hat{}, \check{}), \cdots, (A_t, \times, \hat{}, \check{})$ be independent. Let A be any subdirect sum with identity of* (*not necessarily finite*) *subdirect powers of A_i $(i = 1, \cdots, t)$. Then A is a ring-logic* (mod N).

Now, it is well known (see [2; 4]) that every p-ring (p prime) is isomorphic to a subdirect power of F_p, and every p^k-ring (p prime) is isomorphic to a subdirect power of F_{p^k}. Hence, by letting $t = 1$ and $A_1 = F_p$ (respectively, F_{p^k}) in Theorem 3′, we obtain the following corollary (compare with [1; 2]).

COROLLARY. *Any p-ring with identity, as well as any p^k-ring with identity, is a ring-logic* (mod N).

In conclusion, I wish to express my gratitude to the referee for his valuable suggestions.

REFERENCES

1. A. L. Foster, *p-rings and ring-logics*, University California Publ., **1** (1951), 385-396.
2. ———, *p^k-rings and ring-logics*, Ann. Scu. Norm. Pisa, **5** (1951), 279-300.
3. ———, *Unique subdirect factorization within certain classes of universal algebras*, Math. Z., **62** (1955), 171-188.
4. N. H. McCoy and D. Montgomery, *A representation of generalized Boolean riugs*, Duke Math. J., **3** (1937), 455-459.
5. N. H. McCoy, *Rings and Ideals*, Carus Math Monog., **8** (1947).
6. M. H. Stone, *The theory of representations of Boolean algebras*, Trans. Amer. Math. Soc., **40** (1936), 37-111.
7. A. Yaqub, *On the theory of ring-logics*, Can. J. Math., **8** (1956), 323-328.

UNIVERSITY OF CALIFORNIA, SANTA BARBARA