An. Şt. Univ. Ovidius Constanţa Vol. 19(3), 2011, 175–194

Proto-Boolean rings

Sergiu Rudeanu

Abstract

We introduce the family of R-based proto-Boolean rings associated with an arbitrary commutative ring R. They generalize the proto-Boolean algebra devised by Brown [4] as a tool for expressing in modern language Boole's research in *The Laws of Thought*. In fact the algebraic results from [4] are recaptured within the framework of proto-Boolean rings, along with other theorems. The free Boolean algebras with a finite or countable set of free generators, and the ring of pseudo-Boolean functions, used in operations research for problems of 0–1 optimization, are also particular cases of proto-Boolean rings.

The deductive system in Boole's *Laws of Thought* [3] involves both an algebraic calculus and a "general method in Logic" making use of this calculus. Of course, Boole's treatises do not conform to contemporary standards of rigour; for instance, the modern concept of *Boolean algebra* was in fact introduced by Whitehead [12] in 1898; see e.g. [9].

Several authors have addressed the problem of presenting Boole's creation in modern terms. Thus Beth [1], Section 25 summarizes the approach of Hoff-Hansen and Skolem, who describe the algebra devised by Boole as the quotient of an algebra of polynomial functions by the ideal generated by $x^2 - x, y^2 - y, z^2 - z, \ldots$. Undoubtedly the most comprehensive analysis of the *Laws of Thought* is that offered by Hailperin [5] in terms of multisets. Quite recently, Brown [4], taking for granted the existence of formal entities described as polynomials with integer coefficients, subject to the usual computation rules except that the indeterminates are idempotent ($x_i^2 = x_i$), analyses Chapters V-X of [3] within this elementary framework, which he calls *proto-Boolean algebra*.

Key Words: Boole, proto-Boolean algebra, proto-Boolean ring
Mathematics Subject Classification: 03G05, 03G99, 06E20, 13B25, 01A55

The starting point of this paper had been the simple idea of applying the factorization technique recalled above in order to obtain an actual construction of Brown's polynomials, using the conventional ring $R[X]$ with arbitrary X. Then it ocurred to us that even $R[X]$ can be obtained by a similar factorization technique from a more general structure $R[[S]]$, known as a monoidal ring, which in its turn can be constructed as a ring of functions from S to R. Summarizing, proto-Boolean algebra can be obtained with no existential postulate at all. As a matter of fact, the above strategy has pushed us much farther: the properties established in [4] are valid in a much larger class of rings, having also other interesting properties. This will be shown in the present paper, which is structured as follows.

Section 1 introduces $R[[S]]$ as a ring of functions from S to R; a few properties used in the sequel are pointed out. Then we take an arbitrary alphabet Ξ and specialize $S := \Xi^*/\sim$, where $\sim$ is the monoid congruence of Ξ^* which identifies each xy with yx. We thus obtain the conventional polynomial ring $R[\Xi] = R[[\Xi^*/\sim]]$ (cf. Proposition 1.5). Further we specialize $S := (\Xi^*/\sim)/\approx$, where $\approx$ is the monoid congruence of $\Xi^*/\sim$ which identifies each x^2 with x, and prove that $R[[(\Xi^*)/\sim)/\approx]]$ is the ring of R-polynomials in a set of idempotent variables of the same cardinality as Ξ (cf. Proposition 1.7). Now several specializations of the set Ξ provide an increasing sequence of commutative rings

$$R < RP_1 < RP_2 < \cdots < RP_n < \cdots < RP \ ,$$

which we call *proto-Boolean rings*. In particular $\mathbb{Z}P_n$ is Brown's proto-Boolean algebra, while $\mathbb{R}P_n$ turns out to be in bijection with the ring of pseudo-Boolean functions, which has important applications in operations research.

In Section 2 we prove some properties of proto-Boolean rings and we point out the consequences of the following specializations of the ring R: a ring of characteristic 2, a Boolean ring, and the ring $\mathbb{Z}_2$. Thus the ring $\mathbb{Z}_2P_n$ (the ring $\mathbb{Z}_2P$) is the n-generated (the countably generated) free Boolean ring (cf. Theorem 2.4).

Section 3 focuses on the ring RP_n. We study in some detail the set $I = \{p \in RP_n \mid p^2 = p\}$ of idempotents. The results of this Section, along with Theorem 2.1, recapture within the genearal framework RP_n the results of [4] which describe Boole's original algebra*.

All the rings in this paper are associative and with unit.

*Paper [4] presents also Boole's "general method of logic".

1 Construction of proto-Boolean rings

We begin our construction of proto-Boolean rings with an algebra $R[[S]]$ which was pointed out to us by P. Flondor.

Let R be a *commutative ring* and S a *monoid*, whose operation and unit are denoted by concatenation and e, respectively.

It is plain that the set $R^S = \{f \mid f : S \longrightarrow R\}$ *is an* R*-module* with respect to the operations

$$f + g : S \longrightarrow R, \quad (f+g)(s) = f(s) + g(s) \,, \tag{1}$$

$$af : S \longrightarrow R, \quad (af)(s) = af(s) \,. \tag{2}$$

For each $s \in S$ we define $\delta_s \in R^S$ by

$$\delta_s(t) = \begin{cases} 1, & \text{if } t = s \\ 0, & \text{if } t \neq s \end{cases} \tag{3}$$

and we are interested in the *submodule* $R[[S]]$ *of* R^S *generated by the family* $(\delta_s)_{s\in S}$. We will prove that it consists of all the finite linear combinations $\sum_{s\in F} a_s\delta_s$, where $a_s \in R\,(\forall\, s \in S)$ and F is a finite subset of S. It follows from (1)-(3) that

$$(a\delta_s)(t) = \begin{cases} a, & \text{if } t = s \\ 0, & \text{if } t \neq s \end{cases} \quad , \quad (\sum a_s\delta_s)(t) = \begin{cases} a_t, & \text{if } t \in F \\ 0, & \text{if } t \notin F \end{cases} \quad ; \tag{4}$$

in particular $(0\delta_s)(t) = 0$ for all t.

We associate with each family $(a_s)_{s\in F}$ the elements

$$\overline{a_s}^F = \begin{cases} a_s, & \text{if } s \in F \\ 0, & \text{if } s \notin F \end{cases} \,,$$

which have the property $\sum_{s\in F} a_s\delta_s = \sum_{s\in G} \overline{a_s}^F\delta_s$ for every finite set $G \supseteq F$.

Proposition 1.1. $R[[S]]$ *consists of all the functions which can be written in the form* $\sum_{s\in F} a_s\delta_s$*, with the operations*

$$\begin{aligned} &\textstyle\sum_{s\in F} a_s\delta_s + \sum_{s\in G} b_s\delta_s \\ &= \textstyle\sum_{s\in F\cap G}(a_s + b_s)\delta_s + \sum_{s\in F\setminus G} a_s\delta_s + \sum_{s\in G\setminus F} b_s\delta_s = \sum_{s\in F\cup G}(\overline{a_s}^F + \overline{b_s}^G)\delta_s \,, \end{aligned} \tag{5}$$

$$a\textstyle\sum_{s\in F} a_s\delta_s = \sum_{s\in F}(aa_s)\delta_s \,. \tag{6}$$

PROOF: The first equality (5) follows by (1). The second equality is obtained by computing the values of each side at a point $t \in F \cup G = (F \cap G) \cup (F \setminus G) \cup (G \setminus F)$. □

Remark 1.1. In particular $\sum_{s\in F} a_s\delta_s + \sum_{s\in F} b_s\delta_s = \sum_{s\in F}(a_s+b_s)\delta_s$. This identity can be viewed as combining like terms.

Proposition 1.2. *$R[[S]]$ is a ring with respect to the operations* (5) *and*

$$\begin{aligned}(\textstyle\sum_{s\in F} a_s\delta_s)(\sum_{s\in G} b_s\delta_s) &= \textstyle\sum_{t\in F,u\in G}(a_tb_u)\delta_s \\ &= \textstyle\sum_{s\in FG}(\sum\{a_tb_u \mid t\in F, u\in G, tu=s\})\delta_s\ ,\end{aligned} \tag{7}$$

where $FG = \{tu \mid t \in F, u \in G\}$, with zero $\mathbf{0} = 0\delta_e$ and unit $\mathbf{1} = 1\delta_e$.

PROOF: The first equality (7) is a consistent definition because the set FG is finite. To prove the second equality (7) we compute the value of each side at a point $w \in S$. If $w \notin FG$ both values are 0. If $w \in FG$ then

$$(\sum_{t\in F,u\in G}(a_tb_t)\delta_{tu})(w) \overset{(1)}{=} \sum_{t\in F,u\in G}((a_tb_u)\delta_{tu})(w)$$

$$\overset{(4)}{=} \sum\{a_tb_u \mid t\in F, u\in G, tu=w\}$$

$$\overset{(4)}{=} (\sum_{s\in FG}(\sum\{a_tb_u \mid t\in F, u\in G, tu=s\})\delta_s)(w)\ .$$

Further we check here only associativity and left distributivity. Take $\mathbf{a} = \sum_{s\in F} a_s\delta_s, \mathbf{b} = \sum_{s\in G} b_s\delta_s, \mathbf{c} = \sum_{s\in H} c_s\delta_s$. Then it follows easily that

$$(\mathbf{ab})\mathbf{c} = \mathbf{a}(\mathbf{bc}) = \sum_{t\in F,u\in G,v\in H}(a_tb_vc_u)\delta_{tuv}\ .$$

Besides,

$$\mathbf{a}(\mathbf{b}+\mathbf{c}) = (\sum_{t\in F} a_t\delta_t)(\sum_{u\in G\cup H}(\overline{b_u}^G + \overline{c_u}^H)\delta_u)$$

$$= \sum_{t\in F,u\in G\cup H} a_t\overline{b_u}^G\delta_{tu} + \sum_{t\in F,u\in G\cup H} a_t\overline{c_u}^H\delta_{tu}\ .$$

Taking into account that $G \cup H = G \cup (H \setminus G)$, we obtain

$$\sum_{t\in F,u\in G\cup H} a_t\overline{b_u}^G\delta_{tu} = \sum_{t\in F,u\in G} a_t\overline{b_u}^G\delta_{tu} + \sum_{t\in F,u\in H\setminus G} a_t\overline{b_u}^G\delta_{tu} = \mathbf{ab}$$

because $\overline{b_u}^G = 0$ for $u \in H \setminus G$; similarly $\sum_{t\in F,u\in G\cup H} a_t\overline{c_u}^H\delta_{tu} = \mathbf{ac}$. □

Remark 1.2. $\mathbf{0}(s) = 0$ for all s, $\mathbf{1}(e) = 1$ and $\mathbf{1}(s) = 0$ for $s \neq e$. If $a\delta_s = \mathbf{0}$ then $a = 0$.

Remark 1.3. If the monoid S is commutative, then the ring $R[[S]]$ is commutative and $a\mathbf{ab} = \mathbf{a}(a\mathbf{b}) = (a\mathbf{b})\mathbf{a}$ for all $a \in R$ and $\mathbf{a}, \mathbf{b} \in R[[S]]$.

Proposition 1.3. *The ring R is embedded into $R[[S]]$.*

PROOF: Define $\varepsilon : R \longrightarrow R[[S]]$ by $\varepsilon(a) = a\delta_e = a\mathbf{1}$. Then it is immediately seen that ε is a ring homomorphism and if $\varepsilon(a) = \varepsilon(b)$ then $a = (a\delta_e)(e) = (b\delta_e)(e) = b$, hence ε is injective. Therefore $\varepsilon : R \longrightarrow \varepsilon(R)$ is an isomorphism. □

Corollary 1.1. *In $R[[S]]$ we can unambiguously write a instead of $a\delta_e$.*

Proposition 1.4. *If S is a submonoid of a monoid T, then $R[[S]]$ is a subring of $R[[T]]$.*

PROOF: $R[[S]]$ consists of those elements $\sum_{s\in F} a_s\delta_s \in R[[T]]$ for which $F \subseteq S$. □

Now we specialize S as follows. Consider a non-empty set Ξ which may be infinite. The set Ξ^* of words over the alphabet Ξ is a monoid with respect to concatenation, the unit being the empty word λ (the free monoid generated by Ξ). Let $\sim$ be the *monoid congruence of Ξ^* generated by the relation* $\rho = \{(xy, yx) \mid x, y \in \Xi\}$. Then $S := \Xi^*/\sim$ is a monoid.

Lemma 1.1. *The monoid $\Xi^*/\sim$ is commutative.*

PROOF: It suffices to prove that $w_1xwyw_2 \sim w_1ywxw_2$ for every $w_1, w, w_2 \in \Xi^*/\sim$ and $x, y \in \Xi$. Clearly this reduces further to $xwy \sim ywx$. We proceed by induction on w.

For $w := \lambda$ we have $xy \sim yx$ because $xy\,\rho\,yx$. If the property is true for w, it follows from $xwz \sim zwx$, $xy \sim yx$ and $zwy \sim ywz$ that $xwzy \sim zwxy \sim zwyx \sim ywzx$. □

Now we wish to determine the coset modulo $\sim$ of an element $x \in \Xi$. We will use Theorem 2.1.6 in the monograph by Wechler [11], which describes as follows the congruence $\equiv$ generated by a relation ρ of an arbitrary algebra A (in the sense of universal algebra): $a \equiv b$ iff either $a\,\rho\,b$ or there exist an integer $m \geq 1$ and a sequence $a_0 = a, a_1, \ldots, a_m = b$ of elements of A such that for each $i := 1, \ldots, m$ there exist elements $c_i, d_i \in A$ and a translation τ_i of A such that $c_i\,\rho\,d_i$ and either $a_{i-1} = \tau_i(c_i)$ and $a_i = \tau_i(d_i)$ or $a_{i-1} = \tau_i(d_i)$ and $a_i = \tau_i(c_i)$. We will refer to the sequence $a_0, a_1, \ldots, a_m$ as an $\equiv$*- sequence.*

In the case of a monoid, the translations are the maps of the form $s \mapsto rst$ ([11], page 97).

Lemma 1.2. 1) *The coset modulo* $\sim$ *of an element* $x \in \Xi$ *is* $x/\sim = \{x\}$, *while* $\lambda/\sim = \{\lambda\}$.

2) *The set* $\{\lambda\} \cup \Xi$ *is embedded into* $\Xi^*/\sim$.

PROOF: 1) In view of Theorem 2.1.6 in [11], it is sufficient to prove there is no $\sim$-sequence starting with $a_0 = x$ or $a_0 = \lambda$. Indeed, otherwise we would have $x_1 y_1 \rho\, y_1 x_1$ and either $a_0 = r_1 x_1 y_1 t_1$ or $a_0 = r_1 y_1 x_1 t_1$; both cases are impossible in Ξ^*.

2) It follows from 1) that the map $\lambda \mapsto \lambda/\sim$ and $x \mapsto x/\sim$ is an embedding.

□

Corollary 1.2. *Each element of* $\Xi^*/\sim$ *is either* λ *or it can be written in the form* $x_{i_1}^{n_1} \dots x_{i_k}^{n_k}$, *where* $n_1, \dots, n_k \geq 1$, $x_{i_1}, \dots, x_{i_k} \in \Xi$ *and* $i_1, \dots, i_k$ *are pairwise distinct, the representation being unique up to the order of factors.*

PROOF: An element of $\Xi^*/\sim$ is either λ or of the form $s = \sigma/\sim$, with $\sigma = x_{h_1} \dots x_{h_m} \in \Xi^*$. If $\{i_1, \dots, i_k\}$ are the distinct indices from $\{h_1, \dots, h_m\}$ and x_{i_1} appears n_1 times in $\sigma, \dots, x_{i_k}$ appears n_{i_k} times in σ, then $\sigma \sim \sigma' = x_{i_1}^{n_1} \dots x_{i_k}^{n_k}$.

This representation is unique up to the order of factors, because if $s = \tau/\sim$ then $\sigma \sim \tau$ and the corresponding $\sim$-sequence shows that τ is obtained from σ by a permutation of $x_{h_1}, \dots, x_{h_m}$. hence $s = \tau'/\sim$, where τ' is obtained from σ' by a permutation of $x_{i_1}, \dots, x_{i_k}$.

Finally the desired conclusion is obtained by writing λ instead of $\lambda/\sim$ and $x_{i_1}, \dots, x_{i_k}$ instead of $x_{i_1}/\sim, \dots, x_{i_k}/\sim$, respectively, which is possible by Lemma 1.2. □

In the sequel we will tacitly use Corollary 1.2.

Proposition 1.5. $R[[\Xi^*/\sim]]$ *is the ring* $R[\Xi]$ *of polynomials in the (possibly infinite) set* Ξ *of indeterminates.*

PROOF: This is a paraphrase of Proposition 1.1 and Corollary 1.1 : if we write s instead of δ_s and we identify $a_\lambda \delta_\lambda$ with the element $a_\lambda \in R$ according to Proposition 1.3, then $\sum_{s \in F} a_s \delta_s$ becomes the usual representation of polynomials in $R[\Xi]$. □

Now we are ready to construct polynomials in idempotent indeterminates by using one more factorization. Let $\approx$ be the *monoid congruence of* $\Xi^*/\sim$ *generated by the relation* $\varsigma = \{(x, x^2) \mid x \in \Xi\}$.

Lemma 1.3. 1) *The coset modulo* $\approx$ *of an element* $x_{i_1}^{n_1} \dots x_{i_k}^{n_k} \in \Xi^*/\sim$ *is* $(x_{i_1}^{n_1} \dots x_{i_k}^{n_k})/\approx = \{x_{i_1}^{m_1} \dots x_{i_k}^{m_k} \mid m_1, \dots, m_k \in \mathbb{N} \setminus \{0\}\}$, *while* $\lambda/\approx = \{\lambda\}$.

2) *The coset modulo* $\approx$ *of an element* $x \in \Xi \subset \Xi^*/\sim$ *is* $x/\approx = \{x^n \mid n \in \mathbb{N}, n > 0\}$.

3) *The set* $\{\lambda\} \cup \Xi$ *is embedded into* $(\Xi^*/\sim)/\approx$.

PROOF: 1) Every $\approx$-sequence contains indeterminates, therefore $\lambda/\approx = \{\lambda\}$.

For every $x \in \Xi$ we have $x \varsigma x^2$, hence $x \approx x^2$, therefore $x \approx x^n$ for all $n \geq 1$. This implies

$$x_{i_1}^{n_1} \dots x_{i_k}^{n_k} \approx x_{i_1} \dots x_{i_k} \approx x_{i_1}^{m_1} \dots x_{i_k}^{m_k}$$

for all $n_1, \dots, n_k, m_1, \dots, m_k$. Conversely, let us prove that every $\approx$-sequence starting with $x_{i_1}^{n_1} \dots x_{i_k}^{n_k}$ produces only elements of the form $x_{i_1}^{m_1} \dots x_{i_k}^{m_k}$. Indeed, take an $\approx$-sequence $a_0 = x_{i_1}^{n_1} \dots x_{i_k}^{n_k}, a_1, \dots, a_m$ and suppose $a_{i-1} = x_{i_1}^{m_1} \dots x_{i_k}^{m_k}$. Then $x_i \varsigma y_i = x_i^2$ and either 1) $x_{i_1}^{m_1} \dots x_{i_k}^{m_k} = r_i x_i t_i$ and $a_i = r_i x_i^2 t_i$, or 2) $x_{i_1}^{m_1} \dots x_{i_k}^{m_k} = r_i x_i^2 t_i$ and $a_i = r_i x_i t_i$. In both cases we have $x_i \in \{x_{i_1}, \dots, x_{i_k}\}$ and in view of commutativity we may suppose without loss of generality that $x_i = x_{i_1}$. Therefore in case 1) we have $x_{i_1}^{m_1-1} x_{i_2}^{m_2} \dots x_{i_k}^{m_k} = r_i t_i$ and $a_i = x_{i_1}^{m_1+1} x_{i_2}^{m_2} \dots x_{i_k}^{m_k}$, while case 2) is possible only for $m_1 \geq 2$ and we get $x_{i_1}^{m_1-2} x_{i_2}^{m_2} \dots x_{i_k}^{m_k} = r_i t_i$ and $a_i = x_{i_1}^{m_1-1} x_{i_2}^{m_2} \dots x_{i_k}^{m_k}$ with $m_1 - 1 \geq 1$.

2) follows from 1).

3) The embedding is $\lambda \mapsto \lambda/\approx$ and $x \mapsto x/\approx$. If $x/\approx = y/\approx$ then $\{x^n \mid n \geq 1\} = \{y^n \mid n \geq 1\}$, hence $x = y$. □

Now we specialize $S := (\Xi^*/\sim)/\approx$. We begin with the following corollary of Lemma 1.3.

Corollary 1.3. *Each element of* $(\Xi^*/\sim)/\approx$ *is either* λ *or it can be written in the form* $x_{i_1} \dots x_{i_k}$, *where* $x_{i_1}, \dots, x_{i_k} \in \Xi$ *and* $i_1, \dots, i_k$ *are pairwise distinct, the representation being unique up to the order of factors.*

PROOF: In view of Corollary 1.2, an element of $(\Xi^*/\sim)/\approx$ is either λ or of the form

$$(x_{i_1}^{n_1} \dots x_{i_k}^{n_k})/\approx = (x_{i_1}^{n_1}/\approx) \dots (x_{i_k}^{n_k}/\approx) = (x_{i_1}/\approx) \dots (x_{i_k}/\approx) .$$

If $(x_{i_1}/\approx) \dots (x_{i_k}/\approx) = (y_{j_1}/\approx) \dots (y_{j_h}/\approx)$, it follows that $(x_{i_1} \dots x_{i_k})/\approx = (y_{j_1} \dots y_{j_h})/\approx$, hence $y_{j_1} \dots y_{j_h} \in (x_{i_1} \dots x_{i_k})/\approx$, say $y_{j_1} \dots y_{j_h} = x_{i_1}^{m_1} \dots x_{i_k}^{m_k}$, therefore

$$(y_{j_1}/\approx) \dots (y_{j_h}/\approx) = (x_{i_1}^{m_1})/\approx) \dots (x_{i_k}^{m_k}/\approx) = (x_{i_1}/\approx) \dots (x_{i_k}/\approx) .$$

So, the representation $(x_{i_1}/\approx) \dots (x_{i_k}/\approx)$ is unique up to the order of factors. Finally, Lemma 1.3 also shows that we can unambiguously write λ and $x_{i_1} \dots x_{i_k}$ instead of $\lambda/\approx$ and $(x_{i_1}/\approx) \dots (x_{i_k}/\approx)$. □

In the sequel we tacitly use Corollary 1.3.

Lemma 1.4. *The monoid* $(\Xi^*)/\sim)/\approx$ *is commutative and idempotent.*

PROOF: Commutativity is inherited from $\Xi^*/\sim$. Besides, it is clear that $\lambda^2 = \lambda$ and $(x_{i_1} \dots x_{i_k})^2 = x_{i_1} \dots x_{i_k} x_{i_1} \dots x_{i_k} = x_{i_1}^2 \dots x_{i_k}^2 = x_{i_1} \dots x_{i_k}$. □

Proposition 1.6. *If* $\Xi \subseteq \Upsilon$*, then the monoid* $S = (\Xi^*/\sim)/\approx$ *is a submonoid of* $T = (\Upsilon^*/\sim)/\approx$ *and the ring* $R[[S]]$ *is a subring of* $R[[T]]$*.*

PROOF: It follows from $\Xi^* \subseteq \Upsilon^*$ and Lemma 1.2 that λ and $x \in \Xi \subset \Xi^*$ have the same cosets in $\Xi^*/\sim$ and $\Upsilon^*/\sim$, hence $\Xi^*/\sim$ is a submonoid of $\Upsilon^*/\sim$. This fact and Lemma 1.3 imply that λ and $x \in \Xi \subset \Xi^*/\sim$ have the same cosets in $(\Xi^*/\sim)/\approx$ and $(\Upsilon^*/\sim)/\approx$, therefore $(\Xi^*/\sim)/\approx$ is a submonoid of $(\Upsilon^*/\sim)/\approx$. This fact and Proposition 1.4 imply that $R[[S]]$ is a subring of $R[[T]]$. □

Proposition 1.7. $R[[(\Xi^*/\sim)/\approx]]$ *is the ring of R-polynomials in a set of idempotent variables of the same cardinality as* Ξ*.*

PROOF: As with Proposition 1.5, this is a paraphrase of Proposition 1.1 and Corollary 1.3: we write s instead of δ_s and a_λ instead of $a_\lambda \delta_\lambda$. □

Now we introduce several specializations of Ξ: a countable set $\Xi_\infty = \{x_1, x_2, \dots, x_n, \dots\}$ and the sets $\Xi_1 = \{x_1\}, \Xi_2 = \{x_1, x_2\}, \dots, \Xi_n = \{x_1, \dots, x_n\}, \dots$. Following a suggestion of Brown [4], who calls *proto-Boolean algebra* his modern description of the original algebraic calculus of Boole [2], [3], we introduce the rings $RP_n = R[[(\Xi_n^*/\sim)/\approx]]$, which we call the *n-valued R-based proto-Boolean rings* $(n \in \mathbb{N}, n > 0)$, and $RP = R[[(\Xi_\infty^*/\sim)/\approx]]$, which we call the *complete R-based proto-Boolean ring.*

Theorem 1.1. RP_n *and* RP *are the rings of polynomials in the idempotent indeterminates* $x_1, \dots, x_n$ $(n \in \mathbb{N}, n > 0)$ *and* $\{x_1, x_2, \dots, x_n, \dots\}$*, respectively, and*

$$R < RP_1 < RP_2 < \dots < RP_n < \dots < RP\ ,$$

where $<$ *denotes the relation of being a subring. These rings are commutative.*

PROOF: From Propositions 1.3, 1.6 and 1.7. Commutativity follows from Remark 1.3 and Lemma 1.4. □

Corollary 1.4. $RP = \bigcup_{n\in\mathbb{N}} RPn$*.*

PROOF: It follows from Theorem 1.1 that $\bigcup_{n\in\mathbb{N}} RPn \subseteq RP$. Conversely, take $p = \sum_{s\in F} a_s \delta_s \in RP$. Each δ_s involves a finite number of indeterminates and since F is finite, it follows that only finitely many indeterminates occur in p. So $p \in RPn$ for some n, proving that $p \in \bigcup_{n\in\mathbb{N}} RPn$. □

Corollary 1.5. *For each $p \in RP$, there are infinitely many $n \in \mathbb{N}$ such that $p \in RPn$.*

Remark 1.4. Every ring R is embedded into the proto-Boolean rings RPn ($n \in \mathbb{N}, n > 0$) and RP.

Brown [4] introduces the n-symbol *proto-Boolean algebra* of polynomials with integer coefficients, equipped with "the common (high school) sum, difference and product of polynomials – except that a computed product is made linear in each symbol x_i by application of Boole's law $x_i \times x_i = x_i$". We have just provided an actual construction of this algebra: it is the n-valued $\mathbb{Z}$- based proto-Boolean ring $\mathbb{Z}Pn$, which we will call the *Brown proto-Boolean ring.*

Proto-Boolean rings can also be related to *pseudo-Boolean functions*, which have important applications in operations research, to Boolean programming (MSC 90C09); for the beginning of this field see e.g. the monograph by Hammer and Rudeanu [6]. A pseudo-Boolean function of n variables is any function $f : \{0,1\}^n \longrightarrow \mathbb{R}$. Set $S := (\{x_1, \dots, x_n\}^*/\sim)/\approx$ and define $bij : S \longrightarrow \{0,1\}^n$ by $bij(\lambda) = \varnothing$ and $bij(x_{i_1} \dots x_{i_k}) = (\alpha_1, \dots, \alpha_n)$ where $\alpha_{i_1} = \dots = \alpha_{i_k} = 1$, the other $\alpha_j = 0$. Let $PBF(n)$ be the set of pseudo-Boolean functions of n variables. Then the map $f \mapsto f \circ bij$ establishes a bijection between $PBF(n)$ and $\mathbb{R}Pn$.

We will prove in Section 2 that the $\{0,1\}$-based proto-Boolean rings are in fact free Boolean algebras with n generators and with countably many generators, respectively.

2 Properties of proto-Boolean rings

In this Section we begin the study of the properties of proto-Boolean rings and we point out the consequences of the following specializations of the ring R: a ring of characteristic 2, a Boolean ring, the ring $\mathbb{Z}_2$.

Proposition 2.1. *Each element of RPn can be written as a sum of an element $a_0 \in R$ and a sum of terms of the form $ax_{i_1} \dots x_{i_k}$ with $a \in R$ and pairwise distinct indices $i_1, \dots, i_k$, the subsets $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$ being pairwise distinct.*

PROOF: From Proposition 1.1 and Corollary 1.3. □

Now we introduce in RPn the operation $'$ of *negation* and some supplementary notation:

$$p' = 1 - p,\ p^1 = p,\ p^0 = p'\ \ (p \in RPn)\ , \tag{8}$$

$$X = \{x_1, \ldots, x_n\} \text{ and } X^A = x_1^{\alpha_1} \ldots x_n^{\alpha_n} \text{ for } A = (\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n\ . \tag{9}$$

The following properties hold:

$$A^A = 1 \text{ and } A^B = 0 \text{ if } A \neq B\ , \tag{10}$$

$$X^A X^B = 0 \text{ if } A \neq B \text{ and } X^A X^A = X^A\ , \tag{11}$$

$$\textstyle\sum_{A \in \{0,1\}^n} X^A = 1\ . \tag{12}$$

This is easily checked, as in a Boolean algebra. Note, however, that the proof is based on the idempotency of the elements of X : $xx' = x(1-x) = x - x^2 = 0$, which is not shared by all the elements of RPn.

Theorem 2.1. *Every element of RPn can be written in the form*

$$\textstyle\sum_{A \in \{0,1\}^n} p(A) X^A\ , \tag{13}$$

where all the factors $p(A)$ belong to R and are uniquely determined by p.

PROOF: (as in Boolean algebras). The existence of the representation (13) follows from Proposition 2.1 by introducing in each monoid $x_{i_1} \ldots x_{i_k}$ the missing indeterminates x by the technique

$$x_{i_1} \ldots x_{i_k} = 1 x_{i_1} \ldots x_{i_k} = x x_{i_1} \ldots x_{i_k} + x' x_{i_1} \ldots x_{i_k}\ .$$

To prove uniqueness, suppose $\sum_A p(A) X^A = \sum_A q(A) X^A$, take an arbitrary $B \in \{0,1\}^n$ and multiply by X^B. It follows by (11) that $p(B) X^B = q(B) X^B$, hence $p(B) - q(B) = 0$ by Remark 1.2. □

Corollary 2.1. *For every $p, q \in RPn$ and $A \in \{0,1\}^n$ we have*

$$(p+q)(A) = p(A) + q(A)\ ,$$

$$(pq)(A) = p(A) q(A)\ ,$$

$$p'(A) = (p(A))'\ .$$

PROOF: For instance, the last equality follows from $p' = \sum_A p'(A) X^A$ and

$$p' = 1 - p \overset{(12)}{=} \sum_A 1 X^A - \sum_A p(A) X^A = \sum_A (1 - p(A)) X^A = \sum_A (p(A))' X^A\ .$$

□

Remark 2.1. Theorem 1.1, Corollary 1.4 and Theorem 2.1 show that for every $p \in RP$ and every n such that $p \in RPn$, the element p has a representation of the form (13) for every $m \geq n$. For $m := n+1$, this representation is

$$p = \sum_{\overline{A} \in \{0,1\}^{n+1}} \overline{p}(\overline{A}) \overline{X}^{\overline{A}} ,$$

where: 1) $\overline{A} = (\alpha_1, \ldots, \alpha_n, \alpha_{n+1}) = (A, \alpha_{n+1}) \in \{0,1\}^{n+1}$, with $A = (\alpha_1, \ldots, \alpha_n)$, 2) $\overline{X}^{\overline{A}} = X^A x_{n+1}^{\alpha_{n+1}}$, and 3) $\overline{p}(A,1) = \overline{p}(A,0) = p(A)$.

In the rest of this Section we denote by *P either of the rings RPn and RP.* The set

$$I = \{p \in P \mid p^2 = p\} ,$$

which essentially goes back to Boole, makes the link between proto-Boolean rings and Boolean rings. Recall that a *Boolean ring* is a ring with unit satisfying the identity $x^2 = x$. It is well known that every Boolean ring is commutative and of *characteristic* 2, which means that it satisfies the identity $x+x = 0$. Recall also the equivalence between Boolean rings $(B, +, \cdot, 0, 1)$ and Boolean algebras $(B, \vee, \wedge, ', 0, 1)$, with $x \cdot y = x \wedge y, x \vee y = x+y+xy, x' = 1+x = 1-x$, and $x + y = (x \wedge y') \vee (x' \wedge y)$.

Remark 2.2. The indeterminates and 0,1 belong to I.

In the following we work with the representation (13) of an element $p \in P$; cf. Remark 2.1.

Proposition 2.2. *The following conditions are equivalent for an element $p \in P$:*

(i) $p \in I$;

(ii) $(p(A))^2 = p(A)$ *for all* A .

PROOF: It follows from Corollary 2.1 that $p^2(A) = (p(A))^2$, hence $p \in I \iff p^2 = p \iff (p(A))^2 = p(A)$ for all A. □

Since condition (ii) above can be written in the form $p(A)(1 - p(A)) = 0$, we obtain the following two consequences.

Corollary 2.2. *The ring P has divisors of zero, e.g. the elements of $I \setminus \{0\}$.*

Corollary 2.3. *If the ring R has no divisors of zero, then the following hold:*

(i) $p \in I \iff p(A) \in \{0,1\}$ *for all* $A \in \{0,1\}^n$;

(ii) $ap = 0$ *with* $a \in R$, $p \in P \implies a = 0$ *or* $p = 0$.

PROOF: If $ap = 0$ then $\sum_A ap(A)X^A = 0$. Taking a fixed $B \in \{0,1\}^n$ and multiplying by X^B we get $ap(B)X^B = 0$, hence $ap(B) = 0$ by Remark 1.2. Therefore if $a \neq 0$ it follows that $p(B) = 0$ for all $p \in \{0,1\}^n$, hence $p = 0$. □

Theorem 2.2. *The following conditions are equivalent for P:*

(i) *the ring R is of characteristic* 2 *;*

(ii) *every subring of P is of characteristic* 2 *;*

(iii) *the ring P is of characteristic* 2 *;*

(iv) *I is a subring of P ;*

(v) *I is a Boolean subring of P .*

PROOF: (iii)$\Longrightarrow$(ii)$\Longrightarrow$(ii): Trivial.

(i)$\Longrightarrow$(iii): $p + p = 1p + 1p = (1 + 1)p = 0$.

(iii)$\Longrightarrow$(iv): If $p, q \in I$, then $(pq)^2 = p^2q^2 = pq$, $(p + q)^2 = p^2 + q^2 = p + q$, $(-p)^2 = p^2 = p = -p$.

(iv)$\Longrightarrow$(v): By the definition of I.

(v)$\Longrightarrow$(i): Since $1 \in I$, we have $1 + 1 = 0$. □

Theorem 2.3. *The following conditions are equivalent for P:*

(i) *R is a Boolean ring ;*

(ii) *every subring of P is Boolean ;*

(iii) *P is a Boolean ring*

(iv) $I = P$.

PROOF: (iii)$\Longrightarrow$(ii)$\Longrightarrow$(i): Trivial.

(i)$\Longrightarrow$(iii): The elements $p(A) \in R$ satisfy condition (ii) in Proposition 2.2.

(iii)$\Longleftrightarrow$(iv): Both conditions mean $p^2 = p$ for all $p \in P$. □

Theorem 2.4. *The ring* $\{0,1\}Pn$ *(the ring* $\{0,1\}P$*) is the free Boolean ring with n generators (with countably many generators).*

PROOF: $\{0,1\}Pn$ and $\{0,1\}P$ are Boolean rings by Theorem 2.3

Theorem 2.1 implies that the elements of $\{0,1\}Pn$ are of the form $p = \sum_{A \in \mathbf{F}} X^A$, where $\mathbf{F}$ runs over the subsets of $\{0,1\}^n$, therefore $\{0,1\}Pn$ is generated by the set $\{x_1, \ldots, x_n\}$, hence the Boolean algebra $FB(n)$ equivalent to $\{0,1\}Pn$ is also generated by the set $\{x_1, \ldots, x_n\}$. This set is independent, that is, all $x_{i_1}^{\alpha_1} \ldots x_{i_k}^{\alpha_k} \neq \mathbf{0}$: the reason is that in any ring $R[[S]]$ we have $\delta_s \neq 0$ for all $s \in S$. Therefore $FB(n)$ is the free Boolean algebra with n generators by Theorem 14.2 in [10]. Clearly freeness is transferred to $\{0,1\}Pn$.

For $\{0,1\}P$ the proof is similar, except that n is not fixed, but runs over $\mathbb{N} \setminus \{0\}$, and the set of generators is $\{x_1, x_2, \ldots, x_n, \ldots\}$.

SECOND PROOF for $\{0,1\}Pn$: There are 2^n coefficients $p(A)$ in the representation (13), therefore $\{0,1\}Pn$ has 2^{2^n} elements and the same is true for $FB(n)$. This implies the desired conclusion by Corollary 4.9.7 in [7]. □

3 Transforming the indeterminates into variables

In this section we focus on the ring *RPn, which we denote simply by P*. We prove that P is isomorphic to a ring of functions $f : P^n \longrightarrow P$ and we study in some detail the set $I = \{p \in P \mid p^2 = p\}$ of idempotents. As mentioned by Brown [4], this is justified by the fact that Boole actually worked with idempotent arguments. We will recapture the algebraic results of [4], some of them with different proofs.

Recall first that if R is a (commutative) ring with unit, then the set $R^{R^n} = \{f \mid f : R^n \longrightarrow R\}$, endowed with the pointwise defined operations, i.e, for every $Q \in R^n$,

$$(f+g)(Q) = f(Q) + g(Q),\ (fg)(Q) = f(Q)g(Q),\ 0'(Q) = 0,\ 1'(Q) = 1\ ,$$

is also a (commutative) ring with unit.

In the sequel we use the *notation* $Q = (q_1, \ldots, q_n)$ for the elements of P^n. Note first that identities (11) and (12) extend to

$$(11') \qquad Q^A Q^B = 0 \text{ if } A \neq B \text{ and } Q^A Q^A = Q^A\ (\forall\, A \in \{0,1\}^n)\ \ (\forall\, Q \in I^n)\ ,$$

$$(12') \qquad \textstyle\sum_{A\in\{0,1\}^n} Q^A = 1\ \ (\forall\, Q \in P^n)\ .$$

None of the two identities (11′) can be extended to arbitrary $Q \in P^n$, because $qq' = 0$ only for $q \in I$.

Theorem 3.1. *The map* $^* : P \longrightarrow P^{P^n}$ *defined by*

$$(14) \qquad p^*(q_1, \ldots, q_n) = \textstyle\sum_{A\in\{0,1\}^n} p(A) q_1^{\alpha_1} \ldots q_n^{\alpha_n},\ \textit{where } A = (\alpha_1, \ldots, \alpha_n)\ ,$$

establishes an isomorphism between the rings P *and* $P^* = \{p^* \mid p \in P\}$.

PROOF: Theorem 2.1 shows that the map * is well defined, and using it together with Corollary 2.1, we get $(p_1 + p_2)^*(Q) = p_1^*(Q) + p_2^*(Q) = (p_1^* + p_2^*)(Q)$, hence $(p_1 + p_2)^* = p_1^* + p_2^*$ and similarly $(p_1 p_2)^* = p_1^* p_2^*$. Besides, formula (12′) implies that $1^*(Q) = 1 = \mathbf{1}(Q)$, hence $1^* = \mathbf{1}$. Therefore * is a ring homomorphism and it remains to prove that it is injective.

Indeed, note first that $p^*(A) = p(A)$ for all $A \in \{0,1\}^n$. Hence if $p_1^* = p_2^*$, then $p_1(A) = p_1^*(A) = p_2^*(A) = p_2(A)$ for all A, showing that $p_1 = p_2$. □

Remark 3.1. The following properties are easy to check:

for every $a \in R$, $a^*(Q) = a$ $(\forall\, Q \in P^n)$,

for every $x_i \in X$, $x_i^*(Q) = q_i$ $(\forall\, Q \in P^n)$,

for every $p \in P$, $p^*(A) = p(A)$ $(\forall\, A \in \{0,1\}^n)$,

for every $p \in P$, $p^*(X) = p$.

However the most significant properties are obtained by restricting the argument of p^* to $Q \in I^n$, as was mentioned above.

Caution. In the rest of this paper we assume that *the ring R has no divisors of zero.*

Proposition 3.1. *The following conditions are equivalent for $p \in P$ and $Q \in I^n$:*

(i) $p^*(Q) = 0$ *;*

(ii) $p(A) = 0$ *or* $Q^A = 0$, *for all* $A \in \{0,1\}^n$ *;*

(iii) $p(A)Q^A = 0$, *for all* $A \in \{0,1\}^n$.

PROOF: (ii)$\Longleftrightarrow$(iii): By Corollary 2.3(ii).

(iii)$\Longrightarrow$(i) : By (14).

(i)$\Longrightarrow$(iii): Multiply $\sum_B p(B)Q^B = 0$ by Q^A and use $(11')$. □

Now we establish analogues of the Verification Theorem in Boolean algebras.

Proposition 3.2. *The following conditions are equivalent for $p_1, p_2 \in P$:*

(i) $p_1^*(Q) = 0 \Longrightarrow p_2^*(Q) = 0$, *for all* $Q \in I^n$ *;*

(ii) $p_1^*(A) = 0 \Longrightarrow p_2^*(A) = 0$, *for all* $A \in \{0,1\}^n$.

PROOF: (i)$\Longrightarrow$(ii): Trivial.

(ii) implies that $p_1^*(A) = 0$ or $Q^A = 0$ $(\forall\, A) \Longrightarrow p_2^*(A) = 0$ or $Q^A = 0$, whence (i) follows by Proposition 3.1. □

Corollary 3.1. *The following conditions are equivalent for $p_1, p_2 \in P$:*

(i) $p_1^*(Q) = 0 \Longleftrightarrow p_2^*(Q) = 0$, *for all* $Q \in I^n$ *;*

(ii) $p_1^*(A) = 0 \Longleftrightarrow p_2^*(A) = 0$, *for all* $A \in \{0,1\}^n$.

Theorem 2.1 and Corollary 2.3(i) immediately imply that the following relation is a *partial order on I*:

$$p_1 \leq p_2 \Longleftrightarrow p_1(A) \leq p_2(A)\ (\forall\, A \in \{0,1\}^n)\ . \tag{15}$$

In particular $p \geq 0$ iff $p(A) \geq 0$ $(\forall\, A \in \{0,1\}^n$.

Proposition 3.3. *The following conditions are equivalent for $p_1, p_2 \in I$:*

(i) $p_1 \leq p_2$;

(ii) $\forall\, Q \in I^n :\ (p_2^*(Q) = 0 \Longrightarrow p_1^*(Q) = 0)$;

(iii) $\forall\, Q \in I^n :\ (p_2^*)'(Q)p_1^*(Q) = 0$.

PROOF: Note that $p_1^*(A), p_2^*(A) \in \{0,1\}$ by Corollary 2.3 and Remark 3.1. Hence, according to (15), $p_1 \leq p_2$ if and only if $p_2^*(A) = 0 \Longrightarrow p_1^*(A) = 0$ for all $A \in \{0,1\}^n$, therefore (i)$\Longleftrightarrow$(ii) by Proposition 3.2.

Since ab and $a' = 1-a$ are the same for $a, b \in \{0,1\}$ no matter whether they are calculated in $\{0,1\}$ or in P,[†] it also follows that $p_1 \leq p_2 \Longleftrightarrow p_2'(A)p_1(A) = 0$ $(\forall\, A \in \{0,1\}^n)$, while $(p_2^*)'(Q)p_1^*(Q) = \sum_A p_2'(A)p_1(A)Q^A$ by (14) and Corollary 2.1, it also follows that (i)$\Longrightarrow$(iii).

Finally, (iii)$\Longrightarrow$(ii) because (iii) can be written in the form $(p_2^*(Q))'p_1^*(Q) = 0$. □

Now we need the hypothesis that R is an ordered ring. For this concept see e.g. [8]. In such a ring $a^2 \geq 0$ for all a, and if $a, b \geq 0$ then $a + b \geq a$ and $a + b \geq b$, hence $a + b = 0 \Longrightarrow a = b = 0$.

Lemma 3.1. *Suppose R is an ordered ring. If $p_1, \ldots, p_m \in P$ and $p_1, \ldots, p_m \geq 0$, then*

$$\forall\, Q \in I^n :\ \ p_i^*(Q) = 0\ (i = 1, \ldots, m) \Longleftrightarrow \sum_{i=1}^{m} p_i^*(Q) = 0\ .$$

PROOF: It follows from (14) and Remark 3.1 that

$$\sum_{i=1}^{m} p_i^*(Q) = \sum_{i=1}^{m} \sum_{A} p_i^*(A)Q^A = \sum_{A} (\sum_{i=1}^{m} p_i(A))Q^A\ .$$

If $\sum_{i=1}^m p_i^*(Q) = 0$ then multiplication by Q^A yields $(\sum_{i=1}^m p_i(A))Q^A = 0$ for all A. It follows by Corollary 2.3 that for each A we have $\sum_{i=1}^m p_i(A) = 0$ or $Q^A = 0$, and since R is an ordered ring, for each $i \in \{1, \ldots, m\}$ we have $p_i(A) = 0$ or $Q^A = 0$, hence $p_i(A)Q^A = 0$, therefore $p_i^*(A) = 0$ by (14). □

Theorem 3.2. *Suppose R is an ordered ring. Then for every $p_1, \ldots, p_m \in P$,*

$$\forall\, Q \in I^n :\ \ p_i^*(Q) = 0\ (i = 1, \ldots, m) \Longleftrightarrow \textstyle\sum_{i=1}^m (p_i^*)^2(Q) = 0\ . \tag{16}$$

PROOF: Note that $(p^*)^2(A) = (p^*(A))^2 = (p(A))^2 \geq 0$ and apply Lemma 3.1. □

[†] $1 + 1$ need not be the same.

Proposition 3.4. *For every $p \in P, q \in I$ and $Q \in P^{n-1}$,*

$$p^*(q,Q) = 0 \Longleftrightarrow p^*(1,Q)q = p^*(0,Q)q' = 0 \Longrightarrow p^*(0,Q)p^*(1,Q) = 1 \ .$$

PROOF: We have $p^*(q,Q) = p^*(1,Q)q + p^*(0,Q)q'$ by (14), hence $p^*(q,Q) = 0$ implies $p^*(1,Q)q = 0$ and $p^*(0,Q)q' = 0$ by multiplying with q and q'. This implies further $p^*(0,Q)p^*(1,Q)q = p^*(0,Q)p^*(1,Q)q' = 0$ and since $q + q' = 1$ we get $p^*(0,Q)p^*(1,Q) = p^*(0,Q)p^*(1,Q)(q+q') = 0$. □

The following construction is useful in the study of proto-Boolean equations. We associate with each $p \in P$ an element $p_N \in P$, for which we suggest the name *normalized* p, borrowed from the language of Hilbert spaces, and which is defined as follows: for each $A \in \{0,1\}^n$,

$$p_N(A) = \begin{cases} 1, & \text{if } p(A) \neq 0, \\ 0 & \text{if } p(A) = 0. \end{cases}$$

Remark 3.2. $ap_N(A) = 0 \Longleftrightarrow ap(A) = 0$, because if $a \neq 0$ then

$$ap_N(A) = 0 \Longleftrightarrow p_N(A) = 0 \Longleftrightarrow p(A) = 0 \Longleftrightarrow ap(A) = 0 \ .$$

We are interested in equations of the form $p^*(\xi, Q) = 0$, where $p \in P$, and we are looking for solutions of the form $\xi = p_1^*(Q)$ with $p_1 \in P(n-1) \cap I$ (an *interpretable* solution, in Boole's terminology). The meaning of the solution is that $p^*(p_1^*(Q), Q) = 0$ is an identity.

Proposition 3.5. *If $p \in P$ and $p_1 \in P(n-1) \cap I$, then for every $Q \in I^{n-1}$,*

$$p^*(p_1^*(Q), Q) = 0 \Longleftrightarrow p_N^*(p_1^*(Q), Q) = 0 \ .$$

PROOF: By applying in turn Propositions 3.4 and 3.2, via Remarks 3.1 and 3.2, we obtain

$$p^*(p_1^*(Q), Q) = 0 \Longleftrightarrow p^*(1,Q)p_1^*(Q) = p^*(0,Q)(p_1^*)'(Q) = 0$$

$$\Longleftrightarrow \forall\, A \in \{0,1\}^n)\ p(1,A)p_1(A) = 0\ \&\ \forall\, A \in \{0,1\}^n)\ p(0,A)p_1'(A) = 0$$

$$\Longleftrightarrow \forall\, A \in \{0,1\}^n\ p_N(1,A)p_1(A) = 0\ \&\ \forall\, A \in \{0,1\}^n\ p_N(0,A)p_1'(A) = 0$$

and the proof is completed by applying the same technique in the opposite sense for p_N. □

Theorem 3.3. *Consider an equation of the form $p^*(\xi, Q) = 0$, where $p \in P$ and $Q \in P^{n-1}$. A necessary and sufficent condition for the existence of an interpretable solution $\xi = p_1^*(Q)$ with $p_1 \in I$, is $p^*(0,Q)p^*(1,Q) = 0$ ($\forall\, Q \in I^{n-1}$.*

PROOF: The condition is necessary by Proposition 3.4. Conversely, if the condition is satisfied, we will prove that $q := p_N^*(0,Q)$ is an interpretable solution. Firstly, $q \in I$ by Corollary 2.3(i). Then

$$p^*(p_N^*(0,Q),Q) = p^*(1,Q)p_N^*(0,Q) + p^*(0,Q)(p_N^*(0,Q))'$$

$$= \sum_{A\in\{0,1\}^{n-1}} S_1(A)Q^A + \sum_{A\in\{0,1\}^{n-1}} S_2(A)Q^A \ ,$$

where $S_1(A) = p^*(1,Q)p_N^*(0,Q)$ and $S_2(A) = p^*(0,Q)(p_N^*)'(0,Q)$. If $p^*(0,Q) = 0$ then $P_N^*(0,Q) = 0$ and $S_1(A) = S_2(A) = 0$. If $p^*(0,Q) \neq 0$ then $p_N^*(0,Q) = 1$ and $S_2(A) = 0$, while the hypothesis implies $p^*(1,Q) = 0$ and $S_1(A) = 0$. Thus $p^*(p_N^*(0,Q),Q) = 0$. □

The partial order (15) on I is transferred by isomorphism (cf. Theorem 3.1) to $I^* = \{p^* \mid p \in I\}$:

$$(15') \qquad p_1^* \leq p_2^* \Longleftrightarrow p_1 \leq p_2 \Longleftrightarrow p_1(A) \leq p_2(A) \ (\forall\, A \in \{0,1\}^n) \ .$$

This suggests the possibility of characterizing the solution by a double inequality, as in a Boolean algebra.

Theorem 3.4. *If an equation $p^*(\xi,Q) = 0$ has interpretable solutions, then these solutions $p_1^*(Q)$ with $p_1 \in I$ are characterized by the condition*

$$p_N^*(0,Q) \leq p_1^*(Q) \leq (p_N^*(1,Q))' \ \ (\forall\, Q \in P^{n-1}) \ .$$

PROOF: By applying Propositions 3.5 and 3.4 we obtain

$$p^*(p_1^*(Q),Q) = 0 \Longleftrightarrow p_N^*(p_1^*(Q),Q) = 0$$

$$\Longleftrightarrow p_N^*(1,Q)p_1^*(Q) = 0 \ \ \&\ \ p_N^*(0,Q)(p_1^*(Q))' = 0 \ .$$

Since $p_1, p_N \in I$, it follows by Theorem 2.1 and (14) that the elements $p_1^*(Q), p_N^*(1,Q)$ and $p_N^*(0,Q)$ are in I, therefore they obey Proposition 3.3. Using this fact and noticing the identity $(p')' = p$, we see that the last two conditions are equivalent to

$$p_1^*(Q) \leq (p_N^*(1,Q))' \ \ \&\ \ p_N(0,Q) \leq p_1^*(Q) \ .$$

□

As in [4], Theorem 3.4 can be refined by introducing *antecedents* and *consequents* of the equation under investigation.

Conclusions The origin of this paper was the desire of providing an actual construction of the proto-Boolean algebra introduced in [4]. Yet we have gone

much farther by introducing the family of proto-Boolean rings, which includes not only the proto-Boolean algebra, but also many Boolean rings. The aim of recapturing the algebraic part of [4] has been achieved; some of the results remain valid for an arbitrary basic ring R, the other require the condition that R is an *integral domain* (i.e., the assumption of non-existence of divisors of zero is added to commutativity). The proto-Boolean algebras are obtained for $R := \mathbb{Z}$.

Acknowledgment. The use of the algebra $R[[S]]$ pointed out by P. Flondor has much improved a previous version of this paper. The comments of F.M. Brown concerning good English usage have been most helpful.

References

[1] Beth, E.W., *The Foundations of Mathematics: A Study in the Philosophy of Sciences*, North-Holland Publ. Co., 1959.

[2] Boole, G., *The Mathematical Analysis of Logic, Being an Essay Towards a Calculus of Deductive Reasoning*, Cambridge 1847. Reprinted by Philosophical Library, New York, 1948; in *Studies in Logic and Probability by George Boole*, Watts & Co., London, 1952; by Basil Blackwell, Oxford, U.K., 1965; by Thoemmess Press, Bristol, U.K., 1998; and by Kessenger Publ., Whitefish, MT, 2007.

[3] Boole, G., *An Investigation of the Laws of Thought, on Which Are Founded the Mathematical Theories of Logic and Probabilities*, Walton, London, 1854. Reprinted by Open Court Publ. Co., Chicago/London, 1911; by Dover Books, New York, 1951; by Prometheus Books, Buffalo, 2003; and by Cosimo Books, New York, 2007.

[4] Brown, F.M., *George Boole's deductive system*. Notre Dame J. Formal Logic, 50(2009), 303-330.

[5] Hailperin, T., *Boole's Logic and Probability*, 2nd edition, North-Holland Publ. Co., 1986.

[6] Hammer, P.L., Rudeanu, S., *Boolean Methods in Operations Research and Related Areas*, Springer-Verlag, New York, 1968.

[7] Koppelberg, S., *Handbook of Boolean Algebras*, vol. 1. Edited by J.D. Monk and R. Bonnet, North-Holland, Amsterdam/New York/Oxford/Tokyo, 1989.

[8] MacLane, S., Birkhoff, G., *Algebra*, MacMillan Co., New York, 1967.

[9] Padmanabhan, R., Rudeanu, S., *Axioms for Lattices and Boolean Algebras*, World Scientific, Singapore, 2008.

[10] Sikorski, R., *Boolean Algebras*, 2nd ed., Springer-Verlag, Berlin/Göttingen /Heidelberg/New York, 1964.

[11] Wechler, W., *Universal Algebra for Computer Scientists*, Springer-Verlag, Berlin/Heidelberg/New York, 1992.

[12] Whitehead, A.N., *A Treatise on Universal Algebra, with Applications*, Cambridge Univ. Press, 1898.

University of Bucharest,

Faculty of Mathematics and Informatics, Str. Academiei 14, 010014 Bucharest,
Romania
e-mail:srudeanu@yahoo.com