Mathematical Structures in Computer Science (2020), **30**, pp. 572–596
doi:10.1017/S0960129519000203

CAMBRIDGE UNIVERSITY PRESS

PAPER

Free Heyting algebra endomorphisms: Ruitenburg's Theorem and beyond

Silvio Ghilardi[1,*] and Luigi Santocanale[2]

[1]Dipartimento di Matematica, Università degli Studi di Milano and [2]LIS, CNRS UMR 7020, Aix-Marseille Université
*Corresponding author. Email: silvio.ghilardi@unimi.it

(Received 03 January 2019; revised 18 October 2019; accepted 24 October 2019; first published online 21 January 2020)

Abstract

Ruitenburg's Theorem says that every endomorphism f of a finitely generated free Heyting algebra is ultimately periodic if f fixes all the generators but one. More precisely, there is $N \geq 0$ such that $f^{N+2} = f^N$, thus the period equals 2. We give a semantic proof of this theorem, using duality techniques and bounded bisimulation ranks. By the same techniques, we tackle investigation of arbitrary endomorphisms of free algebras. We show that they are not, in general, ultimately periodic. Yet, when they are (e.g. in the case of locally finite subvarieties), the period can be explicitly bounded as function of the cardinality of the set of generators.

Keywords: Heyting algebra, Ruitenburg's Theorem, sheaf duality, bounded bisimulations, free algebra endomorphisms

1. Introduction

Unification theory investigates the behavior of substitutions from a syntactic point of view: substitutions are in fact key ingredients in various algorithms commonly used in computational logic. Taking an algebraic point of view, substitutions can be seen as finitely generated free algebra homomorphisms: in fact, such a homomorphism

$$\mu : \mathcal{F}(x_1, \ldots, x_n) \longrightarrow \mathcal{F}(y_1, \ldots, y_m)$$

is uniquely determined by an n-tuple of terms

$$t_1(y_1, \ldots, y_m), \ldots, t_n(y_1, \ldots, y_m)$$

and acts by associating with any term $u(x_1, \ldots, x_n)$ the term

$$u(t_1/x_1, \ldots, t_n/x_n)$$

obtained by substitution. If free algebras are intended not as "absolutely free algebras," but as "free algebras in an equational class E," the same correspondence between homomorphisms and substitutions works, provided terms are intended as equivalence classes of terms modulo E and substitutions themselves are taken modulo E. The above correspondence between free algebra homomorphisms and substitutions is the starting point for the algebraic approaches to E-unification theory, like for instance (Ghilardi 1997; Goguen 1989), where structural information about homomorphisms of finitely generated (and also finitely presented) algebras is widely exploited. In this paper, we want to draw the attention on a surprising behavior that such homomorphisms can have in some algebraic logic contexts. Such behavior is unexpectedly similar to that of functions between finite sets.

© Cambridge University Press 2020

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

To explain what we have in mind, let us recall that an infinite sequence

$$a_1, a_2, \ldots, a_i, \ldots$$

is *ultimately periodic* if there are N and k such that for all $s_1, s_2 \geq N$, we have that $s_1 \equiv s_2 \bmod k$ implies $a_{s_1} = a_{s_2}$. If (N, k) is the smallest (in the lexicographic sense) pair for which this happens, then N and k are, respectively, the *index* and the *period* of the ultimately periodic sequence $\{ a_i \}_i$. Thus, for instance, an ultimately periodic sequence with index N and period 2 looks as follows

$$a_1, \ldots, a_N, a_{N+1}, a_N, a_{N+1}, \ldots$$

A typical example of an ultimately periodic sequence is the sequence of the iterations $\{ f^i \}_i$ of an endofunction f of a finite set. Whenever infinitary data are involved, ultimate periodicity comes often as a surprise.

Ruitenburg's Theorem is in fact a surprising result of this kind. Let us write $A(x, \underline{y})$ to mean that the only propositional letters occurring in the formula A are among $x, \underline{y}$ – with $\underline{y}$ being, say, the tuple $y_1, \ldots, y_n$. Moreover, the slash symbol is used for substitution: e.g. $A(B/x, \underline{y})$ means the formula obtained by replacing all occurrences of the variable x in A by the formula B.

Ruitenburg's Theorem states the following: *take a formula* $A(x, \underline{y})$ *of intuitionistic propositional calculus* (*IPC*) *and consider the sequence* $\{ A^i(x, \underline{y}) \}_{i \geq 1}$ *so defined:*

$$A^1 := A, \ldots, A^{i+1} := A(A^i/x, \underline{y}), \tag{1}$$

then, taking equivalence classes under provable bi-implication in (*IPC*)*, the sequence* $\{ [A^i(x, \underline{y})] \}_{i \geq 1}$ *is ultimately periodic with period 2*. The latter means that there is N such that

$$\vdash_{IPC} A^{N+2} \leftrightarrow A^N. \tag{2}$$

An interesting consequence of this result is that *least (and greatest) fixpoints of monotonic formulae are definable in* (*IPC*) (Ghilardi et al. 2016, 2019; Mardaev 2007, 1993): this is because the sequence (1) becomes increasing when evaluated on $\bot/x$ (if A is monotonic in x), so that the period is decreased to 1. Thus, the index of the sequence becomes a finite upper bound for the fixpoint approximations convergence: in fact, we have $\vdash_{IPC} A^N(\bot/x) \to A^{N+1}(\bot/x)$ and $\vdash_{IPC} A^{N+1}(\bot/x) \to A^{N+2}(\bot/x)$ by the monotonicity of A, yielding $\vdash_{IPC} A^N(\bot/x) \leftrightarrow A^{N+1}(\bot/x)$ by (2).

Ruitenburg's Theorem was shown in Ruitenburg (1984) via a rather involved purely syntactic proof. The proof has been recently formalized inside the proof assistant COQ by T. Litak, see https://git8.cs.fau.de/redmine/projects/ruitenburg1984. In this paper, we supply a semantic proof, using duality and bounded bisimulation machinery.

Bounded bisimulations are a standard tool in nonclassical logics (Fine 1985) used to characterize satisfiability of bounded depth formulae and hence definable classes of models: examples of the use of bounded bisimulations include for instance (Ghilardi 2000; Ghilardi and Zawadowski 2002; Shavrukov 1993; Visser 1996).

Duality has a long tradition in algebraic logic, see e.g. Esakia (1974) for the case of Heyting algebras. Indeed, many phenomena look more transparent whenever they are analyzed in the dual categories. This especially happens when dualities can convert coproducts and colimits constructions into more familiar honest (i.e. set-theoretic) products and limits constructions. The duality we use to tackle Ruitenburg's Theorem, firstly described in Ghilardi and Zawadowski (1997), see also Ghilardi and Zawadowski (2002), realizes this conversion. It has a mixed geometric/combinatorial nature. In fact, the geometric environment shows *how to find* relevant mathematical structures (products, equalizers, images, ...) using their standard definitions in

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

sheaves and presheaves; on the other hand, the combinatorial aspects show that such constructions *are definable*, thus meaningful from the logical side. In this sense, notice that we work with finitely presented algebras, and our combinatorial ingredients (Ehrenfeucht-Fraissé games, etc.) replace the topological ingredients which are common in the algebraic logic literature (working with arbitrary algebras instead). Duality, although not always in an explicitly mentioned form, is also at the heart of the finitarity results for E-unification theory in Ghilardi (1999, 2000, 2004).

The paper is organized as follows. In Section 2, we show how to formulate Ruitenburg's Theorem in algebraic terms and how to prove it via duality in the easy case of classical logic (where index is always 1). This section supplies the methodology we shall follow in the whole paper. We introduce in Section 3 the required duality ingredients for finitely presented Heyting algebras, leading to the statement of the duality Theorem. The full proof of this theorem appears in the following Section 4. We show then, in Section 5, how to extend the basic argument of Section 2 to finite Kripke models of intuitionistic logic. This extension does not directly give Ruitenburg's Theorem, because it supplies a bound for the indexes of our sequences which is dependent on the poset a given model is based on. Using the ranks machinery introduced in Section 6, this bound is made uniform in Section 7, thus finally reaching our first goal. Having established Ruitenburg's Theorem, we wonder how general this ultimately periodic behavior is among the finitely generated free Heyting algebra endomorphisms and, in Section 8, we supply a counterexample showing that this behavior fails whenever at least two free generators are moved by the endomorphism. In the final Section 9, we prove that, whenever an endomorphism is ultimately periodic, its period can be bound as a function of the number of the free generators only. This observation is used to provide bounds of periods of free algebra endomorphisms in locally finite varieties of Heyting algebras. We present concluding remarks and some open problems in the last section.

Most of the material of this paper was presented at the conference AiML 18 (see Ghilardi and Santocanale 2018); the content of the last two sections as well as a strengthening of the duality theorem of Ghilardi and Zawadowski (1997), however, are novel.

2. The Case of Classical Logic

We explain our methodology in the much easier case of classical logic. In classical propositional calculus (*CPC*), Ruitenburg's Theorem holds with index 1 and period 2, namely given a formula $A(x, \underline{y})$, we prove that

$$\vdash_{CPC} A^3 \leftrightarrow A \tag{3}$$

holds, where A^3 is defined as in (1).

2.1 The algebraic reformulation

First, we transform the above statement (3) into an algebraic statement concerning free Boolean algebras. We let $\mathcal{F}_B(\underline{z})$ be the free Boolean algebra over the finite set $\underline{z}$. Recall that $\mathcal{F}_B(\underline{z})$ is the Lindenbaum–Tarski algebra of classical propositional calculus restricted to a language having just the $\underline{z}$ as propositional variables.

Similarly, morphisms $\mu : \mathcal{F}_B(x_1, \ldots, x_n) \longrightarrow \mathcal{F}_B(\underline{z})$ bijectively correspond to n-tuples of equivalence classes of formulae $A_1(\underline{z}), \ldots, A_n(\underline{z})$ in $\mathcal{F}_B(\underline{z})$: the map μ corresponding to the tuple $A_1(\underline{z}), \ldots, A_n(\underline{z})$ associates with the equivalence class of $B(x_1, \ldots, x_n)$ in $\mathcal{F}_B(x_1, \ldots, x_n)$ the equivalence class of $B(A_1/x_1, \ldots, A_n/x_n)$ in $\mathcal{F}_B(\underline{z})$.

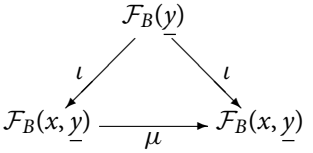
Composition is substitution, in the sense that if $\mu : \mathcal{F}_B(x_1, \ldots, x_n) \longrightarrow \mathcal{F}_B(\underline{z})$ is induced, as above, by $A_1(\underline{z}), \ldots, A_n(\underline{z})$ and if $\nu : \mathcal{F}_B(y_1, \ldots, y_m) \longrightarrow \mathcal{F}_B(x_1, \ldots, x_n)$ is induced by $C_1(x_1, \ldots, x_n), \ldots, C_m(x_1, \ldots, x_n)$, then the map $\mu \circ \nu : \mathcal{F}_B(y_1, \ldots, y_m) \longrightarrow \mathcal{F}_B(\underline{z})$ is induced by the m-tuple $C_1(A_1/x_1, \ldots, A_n/x_n), \ldots, C_m(A_1/x_1, \ldots, A_n/x_n)$.

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

How to translate the statement (3) in this setting? Let $\underline{y}$ be $y_1, \ldots, y_n$; we can consider the map $\mu_A : \mathcal{F}_B(x, y_1, \ldots, y_n) \longrightarrow \mathcal{F}_B(x, y_1, \ldots, y_n)$ induced by the $n+1$-tuple of formulae $A, y_1, \ldots, y_n$, then, taking in mind that in Lindenbaum algebras identity is modulo provable equivalence, the statement (3) is equivalent to

$$\mu_A^3 = \mu_A. \tag{4}$$

This raises the question: which endomorphisms of $\mathcal{F}_B(x, \underline{y})$ are of the kind μ_A for some $A(x, \underline{y})$? The answer is simple: consider the "inclusion" map ι of $\mathcal{F}_B(\underline{y})$ into $\mathcal{F}_B(x, \underline{y})$ (this is the map induced by the n-tuple $y_1, \ldots, y_n$): the maps $\mu : \mathcal{F}_B(x, \underline{y}) \longrightarrow \mathcal{F}_B(x, \underline{y})$ that are of the kind μ_A are precisely the maps μ such that $\mu \circ \iota = \iota$, i.e. those for which the triangle

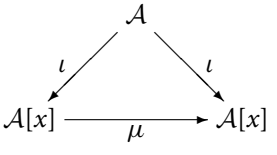


commutes.

It is worth making a little step further: since the free algebra functor preserves coproducts, we have that $\mathcal{F}_B(x, \underline{y})$ is the coproduct of $\mathcal{F}_B(\underline{y})$ with $\mathcal{F}_B(x)$ – the latter being the free algebra on one generator. In general, let us denote by $\mathcal{A}[\underline{x}]$ the coproduct of the Boolean algebra $\mathcal{A}$ with the free algebra on one generator (let us call $\mathcal{A}[x]$ the *algebra of polynomials* over $\mathcal{A}$).

Recall that an algebra is *finitely presented*, if it is isomorphic to the quotient of a finitely generated free algebra by a finitely generated congruence. For Boolean algebras, being "finitely presented" is equivalent to being "finite." Yet, we should keep in mind in the following sections that this equivalence fails for Heyting algebras – so the two notions are in general distinct. A slight generalization of statement (4) now reads as follows:

– let $\mathcal{A}$ be a finitely presented Boolean algebra and let the map $\mu : \mathcal{A}[x] \longrightarrow \mathcal{A}[x]$ commute with the coproduct injection $\iota : \mathcal{A} \longrightarrow \mathcal{A}[x]$



Then, we have

$$\mu^3 = \mu. \tag{5}$$

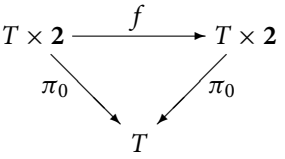
2.2 Duality

The gain we achieved with statement (5) is that the latter is a purely categorical statement, so that we can reinterpret it in dual categories. In fact, a good duality may turn coproducts into products and make our statement easier – if not trivial at all.

Finitely presented Boolean algebras are dual to finite sets; the duality functor maps coproducts into products and the free Boolean algebra on one generator to the two-element set $\mathbf{2} = \{0, 1\}$ (which, by chance is also a subobject classifier for finite sets). Thus, statement (5) now becomes

– let T be a finite set and let the function $f : T \times \mathbf{2} \longrightarrow T \times \mathbf{2}$ commute with the product projection $\pi_0 : T \times \mathbf{2} \longrightarrow T$

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

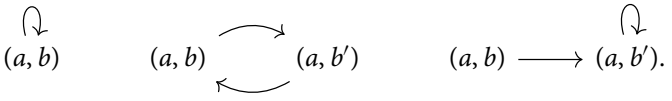


Then, we have

$$f^3 = f. \tag{6}$$

In this final form, statement (6) is now just a trivial exercise, which is solved as follows. Notice first that f can be decomposed as $\langle \pi_0, \chi_S \rangle$ (incidentally, χ_S is the characteristic function of some $S \subseteq T \times \mathbf{2}$). Now, if $f(a,b) = (a,b)$, we trivially have also $f^3(a,b) = f(a,b)$; suppose then $f(a,b) = (a,b') \neq (a,b)$. If $f(a,b') = (a,b')$, then $f^3(a,b) = f(a,b) = (a,b')$, otherwise $f(a,b') = (a,b)$, since there are only two values for b, and even in this case $f^3(a,b) = f(a,b)$.

Let us illustrate these cases by thinking of f as an action of the monoid of natural numbers on the set $A \times \mathbf{2}$, i.e. as a one-letter deterministic automaton:



On each connected component of the automaton, the pair index/period is among $(0,1)$, $(0,2)$, $(1,1)$. We can compute the global index/period of f by means of a max /lcm formula: $(1,2) = (\max\{0,0,1\}, \mathrm{lcm}\{1,2\})$.

3. Duality for Heyting Algebras

In this section, we supply definitions, notation, and statements from Ghilardi and Zawadowski (2002) concerning duality for finitely presented Heyting algebras.

A partially ordered set (poset, for short) is a set endowed with a reflexive, transitive, antisymmetric relation (to be always denoted with $\leq$). A poset P is rooted if it has a greatest element, that we shall denote by $\rho(P)$. If a finite poset L is fixed, we call an *L-evaluation* or simply an *evaluation* a pair $\langle P, u \rangle$, where P is a rooted finite poset and $u : P \longrightarrow L$ is an order-preserving map.

Evaluation *restrictions* are introduced as follows. If $\langle P, u \rangle$ is an L-evaluation and if $p \in P$, then we shall denote by u_p the L-evaluation $\langle \downarrow p, u \circ i \rangle$, where $\downarrow p = \{ p' \in P \mid p' \leq p \}$ and $i : \downarrow p \subseteq P$ is the inclusion map; briefly, u_p is the restriction of u to the downset generated by p.

Evaluations have a strict relationship with finite Kripke models, let us illustrate in detail this connection. If $\langle L, \leq \rangle$ is $\langle \mathcal{P}(\underline{x}), \supseteq \rangle$ (where $\underline{x} = x_1, \ldots, x_n$ is a finite list of propositional letters), then an L-evaluation $u : P \longrightarrow L$ is called a *Kripke model* for the propositional intuitionistic language built up from $\underline{x}$.[1] Given such a Kripke model u and an IPC formula $A(\underline{x})$, the *forcing* relation $u \models A$ is inductively defined as follows:

$$\begin{aligned}
&u \models x_i && \text{iff } x_i \in u(\rho(P)) \\
&u \not\models \bot && \\
&u \models A_1 \wedge A_2 && \text{iff } (u \models A_1 \text{ and } u \models A_2) \\
&u \models A_1 \vee A_2 && \text{iff } (u \models A_1 \text{ or } u \models A_2) \\
&u \models A_1 \to A_2 && \text{iff } \forall p \in P\, (u_p \models A_1 \Rightarrow u_p \models A_2).
\end{aligned}$$

We define for every $n \in \omega$ and for every pair of L-evaluations u and v, the notions of being *n-equivalent*, written $u \sim_n v$. We also define, for two L-evaluations u, v, the notion of being *infinitely equivalent*, written $u \sim_\infty v$.

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

Let $u : P \longrightarrow L$ and $v : Q \longrightarrow L$ be two L-evaluations. The *game* we are interested in has two players, Player 1 and Player 2. Player 1 can choose either a point in P or a point in Q and Player 2 must answer by choosing a point in the other poset. The only rule of the game is that, if $\langle p \in P, q \in Q\rangle$ is the last move played so far, then in the successive move the two players can only choose points $\langle p', q'\rangle$ such that $p' \leq p$ and $q' \leq q$. If $\langle p_1, q_1\rangle, \ldots, \langle p_i, q_i\rangle, \ldots$ are the points chosen in the game, Player 2 wins iff for every $i = 1, 2, \ldots$, we have that $u(p_i) = v(q_i)$. We say that

- $u \sim_\infty v$ iff *Player 2 has a winning strategy* in the above game with infinitely many moves;
- $u \sim_n v$ (for $n > 0$) iff *Player 2 has a winning strategy* in the above game with n moves, i.e. he has a winning strategy provided, we stipulate that the game terminates after n moves;
- $u \sim_0 v$ iff $u(\rho(P)) = v(\rho(Q))$, where we recall that $\rho(P)$, $\rho(Q)$ denote the roots of P, Q.

Notice that $u \sim_n v$ always implies $u \sim_0 v$, by the fact that L-evaluations are order-preserving. We shall use the notation $[v]_n$ for the equivalence class of an L-valuation v via the equivalence relation $\sim_n$.

The following proposition provides an elementary recursive characterization of the relations $\sim_n$, $n \geq 1$. Keeping the above definition for $\sim_0$ as base case for recursion, the proposition supplies an alternative recursive definition for these relations.

Proposition 1. *Given two L-evaluations $u : P \longrightarrow L$, $v : Q \longrightarrow L$, and $n > 0$, we have that $u \sim_{n+1} v$ iff $\forall p \in P\, \exists q \in Q\, (u_p \sim_n v_q)$ and vice versa.*

When $L = \mathcal{P}(x_1, \ldots, x_n)$, the relations $\sim_n$ are related to the implicational degree of the formulas in the language built up from the propositional variables $x_1, \ldots, x_n$. For such an IPC formula $A(\underline{x})$, the implicational degree $d(A)$ is defined as follows:

(i) $d(\bot) = d(x_i) = 0$, for $x_i \in \underline{x}$;
(ii) $d(A_1 * A_2) = \max[d(A_1), d(A_2)]$, for $* = \wedge, \vee$;
(iii) $d(A_1 \to A_2) = \max[d(A_1), d(A_2)] + 1$.

One can prove (Visser 1996) that: (1) $u \sim_\infty v$ holds precisely when $(u \models A \Leftrightarrow v \models A)$ holds for all formulae $A(\underline{x})$; (2) for all n, $u \sim_n v$ holds precisely when $(u \models A \Leftrightarrow v \models A)$ holds for all formulae $A(\underline{x})$ with $d(A) \leq n$. That is, two evaluations are $\sim_\infty$-equivalent iff they force the same formulas and they are $\sim_n$-equivalent iff they force the same formulas up to implicational degree n. Let us remark that, for (1) to be true, it is essential that our evaluations are defined over *finite* posets.

The above discussion motivates a sort of identification of formulae with sets of evaluations closed under restrictions and under $\sim_n$ for some n. Thus, *bounded bisimulations* (this is the way the relations $\sim_n$ are sometimes called) supply the combinatorial ingredients for our duality. For the picture to be complete, we also need a geometric environment, which we introduce using presheaves.

Recall that a poset can be viewed as a topological space whose open subsets are the downward closed subsets. A map between posets is said to be *open* if it is continuous and open in the topological sense. Thus, $f : Q \longrightarrow P$ is open iff it is order-preserving and, for all $q \in Q$ and $p \in P$,

$$p \leq f(q) \;\Rightarrow\; \exists q' \in Q\, (q' \leq q \,\&\, f(q') = p).$$

Let us recall that open surjective maps are called p-morphisms in the standard nonclassical logics terminology.

Let $\mathbf{P_0}$ be the category of finite rooted posets and open maps between them; a *presheaf* over $\mathbf{P_0}$ is a contravariant functor from $\mathbf{P_0}$ to the category of sets and functions, i.e. a functor $H : \mathbf{P_0}^{op} \longrightarrow \mathbf{Set}$. Let us recall what this means: a functor $H : \mathbf{P_0}^{op} \longrightarrow \mathbf{Set}$ associates with each finite rooted poset P

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

a set $H(P)$; if $f : Q \longrightarrow P$ is an open map, then we are also given a function $H(f) : H(P) \longrightarrow H(Q)$; moreover, identities are sent to identities, while composition is reversed, $H(g \circ f) = H(f) \circ H(g)$.

Our presheaves form a category whose objects are presheaves over $\mathbf{P_0}$ and whose maps are natural transformations. Recall that a natural transformation $\psi : H \longrightarrow H'$ is a collection of maps $\psi_P : H(P) \longrightarrow H'(P)$, indexed by the objects of $\mathbf{P_0}$, such that for every map $f : Q \longrightarrow P$ in $\mathbf{P_0}$, we have $H'(f) \circ \psi_P = \psi_Q \circ H(f)$. Throughout the paper, we shall usually omit the subscript P when referring to the P-component ψ_P of a natural transformation ψ.

The basic example of presheaf we need in the paper is described as follows. Let L be a finite poset and let h_L be the contravariant functor so defined:

- for a finite poset P, $h_L(P)$ is the set of all L-evaluations;
- for an open map $f : Q \longrightarrow P$, $h_L(f)$ takes $v : P \longrightarrow L$ to $v \circ f : Q \longrightarrow L$.

The presheaf h_L is actually a sheaf for the canonical Grothendieck topology over $\mathbf{P_0}$. We will not need this fact,[2] nevertheless we call h_L the *sheaf of L-evaluations* (presheaves of the kind h_L, for some L, are called *evaluation sheaves*).

Notice that if $\psi : h_L \longrightarrow h_{L'}$ is a natural transformation, $v \in h_L(P)$, and $p \in P$, then $\psi(v_p) = (\psi(v))_p$. This is due to the fact that the inclusion $\downarrow p \subseteq P$ is an open map, hence an arrow in $\mathbf{P_0}$. Therefore, we shall feel free to use the unambiguous $\psi(v)_p$ to denote $\psi(v_p) = (\psi(v))_p$.

The notion of *bounded bisimulation index* (*b-index*, for short)[3] takes together structural and combinatorial aspects. We say that a natural transformation $\psi : h_L \longrightarrow h_{L'}$ *has b-index n* if, for every $v : P \longrightarrow L$ and $v' : P' \longrightarrow L$, we have that $v \sim_n v'$ implies $\psi(v) \sim_0 \psi(v')$.

The following proposition lists basic facts about b-indexes. In particular, it ensures that natural transformations having a b-index compose.

Proposition 2. *Let $\psi : h_L \longrightarrow h_{L'}$ have b-index n, then it has also b-index m for every $m \geq n$. Moreover, for every $k \geq 0$, for every $v : P \longrightarrow L$ and $v' : P' \longrightarrow L$, we have that $v \sim_{n+k} v'$ implies $\psi(v) \sim_k \psi(v')$.*

Proof. Suppose that ψ has b-index n; we prove by induction on k that

$$\forall v, v' \ \textit{if} \ v \sim_{n+k} v' \ \textit{then} \ \psi(v) \sim_k \psi(v') \qquad ((*)_k)$$

For $k = 0$, $((*)_k)$ is just the definition of ψ having b-index n. Suppose that $((*)_k)$ holds for some k. Let v, v' be such that $v \sim_{n+k+1} v'$. We shall prove that

$$\forall p \in P \, \exists p' \in P' \ \psi(v)_p \sim_k \psi(v')_{p'}$$

(the converse statement is similar). Fix $p \in P$. Since $v \sim_{n+k+1} v'$, there is $p' \in P'$ such that $v_p \sim_{n+k} v'_{p'}$. Using the inductive assumption and the naturality of ψ, we obtain

$$\psi(v)_p = \psi(v_p) \sim_k \psi(v'_{p'}) = \psi(v')_{p'}$$

as wanted. □

We are now ready to state duality theorems. As it is evident from the discussion in Section 2, it is sufficient to state a duality for the category of finitely generated free Heyting algebras. Although it would not be difficult to give a duality for finitely presented Heyting algebras, we state here only a duality for the intermediate category of Heyting algebras freely generated by a finite bounded distributive lattice. This is indeed sufficient for proving Ruitenburg's Theorem and keeps our argumentation simpler and accessible.

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

Theorem 3. *The category of Heyting algebras freely generated by a finite bounded distributive lattice is dual to the subcategory of presheaves over* $\mathbf{P_0}$ *having as objects the evaluations sheaves and as arrows the natural transformations having a b-index.*

We present a full proof of the above theorem in the next section, where we shall also extend the theorem to all finitely approximable varieties of Heyting algebras.

It is important to notice that in the subcategory mentioned in the above theorem, products are computed as in the category of presheaves. This means that they are computed pointwise, like in the category of sets: in other words, we have that $(h_L \times h_{L'})(P) = h_L(P) \times h_{L'}(P)$ and $(h_L \times h_{L'})(f) = h_L(f) \times h_{L'}(f)$, for all finite posets P and all open maps f. Notice moreover that $h_{L\times L'}(P) \simeq h_L(P) \times h_{L'}(P)$, so we have $h_{L\times L'} \simeq h_L \times h_{L'}$; in addition, the two product projections have b-index 0. The situation strongly contrasts with other kind of dualities, see for example Esakia (1974), where products are difficult to compute. The ease by which products are computed might be seen as the principal reason for tackling a proof of Ruitenburg's Theorem by means of sheaf duality.

As a final information, we need to identify the dual of the free Heyting algebra on one generator:

Proposition 4. *The dual of the free Heyting algebra on one generator is* $h_{\mathbf{2}}$*, where* $\mathbf{2}$ *is the two-element poset* $\{0, 1\}$ *with* $1 \leq 0$.

Indeed, we shall see in the next section that $h_{\mathbf{2}}$ is dual to the Heyting algebra freely generated by the distributive lattice $\mathcal{D}(\mathbf{2})$, the lattice of downsets of the chain $\mathbf{2}$. Since $\mathcal{D}(\mathbf{2})$ – which is a three-element chain – is the free distributive (bounded) lattice on one generator, a standard argument proves that the Heyting algebra freely generated by the distributive lattice $\mathcal{D}(\mathbf{2})$ is itself free on one generator.

4. Proof of the Duality Theorem

We present in this section a proof of Theorem 3. The reader interested in Ruitenburg's Theorem might wish to proceed directly to Section 5.

The material in this section is adapted from Ghilardi and Zawadowski (1997) and the proof of the Duality Theorem follows the same paths. However, a technical improvement in the proof – avoiding the "grafting construction" by means of a smart use of the intermediate relations $\leq_n$ – yields an important widening of the duality theory developed in Ghilardi and Zawadowski (1997). Theorem 17 states a generalized duality that applies to all the subvarieties of Heyting algebras with the "finite model property." This theorem is new.

With each L-evaluation $u : P \longrightarrow L$ and each $n \in \omega$, we associate the set $Type_n(u)$ of $\sim_n$-equivalence classes, $Type_n(u) := \{ [u_p]_n \mid p \in P \}$ – where we recall that $[u_p]_n$ denotes the $\sim_n$-equivalence class of u_p. An important, although simple, fact is given by the following proposition:

Proposition 5. *For a finite poset* L *and* $n \in \omega$*, there are only finitely many equivalence classes of* L*-evaluations with respect to* $\sim_n$.

Proof. This is evident for $n = 0$. For $n > 0$, we argue by induction as follows. By Proposition 1, we have that $u \sim_n v$ iff $Type_{n-1}(u) = Type_{n-1}(v)$, hence there cannot be more non $\sim_n$-equivalent L-evaluations than sets of $\sim_{n-1}$ equivalence classes. □

Let $\mathcal{S}(h_L)$ be the set of subpresheaves S of h_L satisfying the following condition for some $n \geq 0$

$$\forall u : P \longrightarrow L,\ \forall v : Q \longrightarrow L\ (u \in S_P\ \&\ u \sim_n v\ \Rightarrow\ v \in S_Q). \tag{7}$$

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

When the condition above holds, we say that n is a *b-index* for S. Notice that the choice of the naming b-index is consistent with the one used in the previous section. Indeed, for $S \subseteq h_L$, let $\chi : h_L \to h_{\mathbf{2}}$ be defined by $\chi_P(u)(p) = 1$ if and only if $u_p \in S_{\downarrow p}$. If n is a b-index for S, then χ is a natural transformation and n is a b-index for χ. Indeed, $h_{\mathbf{2}}$ is a subobject classifier for subpresheaves that are sheaves for the canonical topology, see page 95 of Ghilardi and Zawadowski (2002).

The definition of $\mathcal{S}(h_L)$ can be given in a slightly different way by introducing the relations $\leq_n$. We put, for $u \in h_L(P)$ and $v \in h_L(Q)$,

(i) $v \leq_0 u$ *iff* $v(\rho(Q)) \leq u(\rho(P))$;
(ii) $v \leq_{n+1} u$ *iff* $\forall q \in Q\, \exists p \in P\, (v_q \sim_n u_p)$.

Lemma 6. *Suppose that $v_1 \sim_n v_2$. Then, we have that $v_1 \leq_n v_2$; moreover, for every w, $v_1 \leq_n w$ holds iff $v_2 \leq_n w$ holds.*

Proof. The first claim is immediate, by applying the definitions (distinguish the case $n = 0$ and the case $n > 0$). The second claim follows from the first one and the fact that $\leq_n$ is trivially seen to be transitive. □

Lemma 7. *$\mathcal{S}(h_L)$ can be equivalently defined as the set of subpresheaves S of h_L satisfying the following condition for some $n \geq 0$*

$$\forall u : P \longrightarrow L,\ \forall v : Q \longrightarrow L\ (u \in S_P\ \&\ v \leq_n u\ \Rightarrow\ v \in S_Q). \tag{8}$$

Proof. Let us call $\mathcal{S}'(h_L)$ the set of subpresheaves S of h_L satisfying condition (8). Clearly, $\mathcal{S}'(h_L) \subseteq \mathcal{S}(h_L)$ since condition (8) implies condition (7): in fact, according to Lemma 6, the relation $\sim_n$ is included in the relation $\leq_n$. For the converse, take $S \in \mathcal{S}(h_L)$ having b-index n; in order to show that $S \in \mathcal{S}'(h_L)$, we show that it satisfies (8) for $n+1$. Let in fact u, v be such that $u \in S_P$ and $v \leq_{n+1} u$. Then, considering the root of the domain of v, we know that there is $p \in P$ such that $v \sim_n u_p$. Since S is a subpresheaf of h_L, $u_p \in S_{\downarrow p}$ and finally $v \in S_Q$ because n is a b-index for S. □

Whenever a subpresheaf S satisfies condition (8) relative to n, we say that S has $\mathrm{b}^{\leq}$-index n. Notice that Lemma 7 does not precisely say that condition (8) is equivalent to condition (7). The above proof shows only that if S has $\mathrm{b}^{\leq}$-index n, then it also has b-index n, and that if S has b-index n, then it has $\mathrm{b}^{\leq}$-index $n+1$. Nevertheless, it can be shown that S has a b-index n iff it has $\mathrm{b}^{\leq}$-index n; however, we will not use this result, since it depends on the "grafting construction," see page 77 of Ghilardi and Zawadowski (1997), which is not available if we move from the variety of Heyting algebras to one of its subvarieties. Depending on the context, we shall make use or not of the equivalent definition for $\mathcal{S}(h_L)$ supplied by Lemma 7.

Let, for every $u : P \to L$ and $n \in \omega$,

$$(\downarrow_n u)_Q := \{\, v : Q \longrightarrow L \mid v \leq_n u \,\}.$$

The next lemma is an immediate consequence of Lemma 7.

Lemma 8. *$\downarrow_n u$ is the least subpresheaf F of h_L having $\mathrm{b}^{\leq}$-index n such that $u \in F(P)$. A subpresheaf of S of h_L has $\mathrm{b}^{\leq}$-index n if and only if, for each $u : P \longrightarrow L$ with $u \in S_P$, $\downarrow_n u \subseteq S$.*

In particular $\downarrow_n u \in \mathcal{S}(h_L)$, for each $u : P \to L$. Notice that the map

$$[u]_n \longmapsto \downarrow_n u$$

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

is well defined (actually, it is also injective) and so, by Proposition 5 and for fixed $n \in \omega$, there exists only a finite number of presheaves of the form $\downarrow_n u$. Since

$$S = \bigcup_{u \in S_P} \downarrow_n u,$$

when $S \in \mathcal{S}(h_L)$ has $\mathrm{b}^{\leq}$-index n, it follows that:

Lemma 9. *Every $S \in \mathcal{S}(h_L)$ of $b^{\leq}$-index n is a finite union of elements of the form $\downarrow_n u$.*

Recall that $Sub(h_L)$ denotes the Heyting algebra of subpresheaves of h_L.

Proposition 10. *$\mathcal{S}(h_L)$ is a sub-Heyting algebra of $Sub(h_L)$.*

Proof. It is easily seen that if S and T have b-index n, then both $S \cap T$ and $S \cup T$ have b-index n. Next, consider the standard characterization of implication in subpresheaves:

$$(S \to T)_P = \{\, u \in (h_L)_P \mid \forall h : Q \longrightarrow P \,(u \circ h \in S_Q \;\Rightarrow\; u \circ h \in T_Q)\,\}\,.$$

Notice that, for any $h : Q \longrightarrow P$ and $u \in (h_L)_P$, we have that $u \circ h \sim_\infty u_p$, where p is $h(\rho(Q))$; as a consequence, since every $U \in \mathcal{S}(h_L)$ has a b-index, we have $u \circ h \in U_Q$ iff $u_p \in U_{\downarrow p}$ for every $U \in \mathcal{S}(h_L)$. Thus, the following is an equivalent description of the implication

$$(S \to T)_P = \{\, u \in (h_L)_P \mid \forall p \in P \,(u_p \in S_{\downarrow p} \;\Rightarrow\; u_p \in T_{\downarrow p})\,\}. \tag{9}$$

From this description, it easily follows that if $S, T \in Sub(h_L)$ have b-index n, then $S \to T$ has b-index $n+1$. □

Let $\mathcal{D}(L)$ denote the distributive lattice of downward closed subsets of L and recall that $\mathcal{D}(L)$ is the Birkhoff dual of the poset L, see Birkhoff (1937) and Davey and Priestley (2002). Notice that there is a lattice embedding $\iota_L : \mathcal{D}(L) \longrightarrow \mathcal{S}(h_L)$ associating with a downward closed subset d of L, the subpresheaf

$$\iota_L(d)_P := \{\, u : P \longrightarrow L \mid u(\rho(P)) \in d\,\}.$$

Thus, for $p \in P$ and $u \in h_L(P)$, we have $u_p \in \iota_L(d)_{\downarrow p}$ iff $u(p) \in d$.

We shall prove that $\mathcal{S}(h_L)$ is the free Heyting algebra generated by the finite distributive lattice $\mathcal{D}(L)$ with ι_L as the canonical embedding.

Lemma 11. *The image of ι_L generates $\mathcal{S}(h_L)$ as a Heyting algebra.*

Proof. Clearly, the elements of $\mathcal{S}(h_L)$ having $\mathrm{b}^{\leq}$-index 0 are exactly the elements of the image of ι_L. Now consider an element having $\mathrm{b}^{\leq}$-index $n+1$; by Lemma 9, it is a finite union of elements of the kind $\downarrow_{n+1} u$. We can express such elements in terms of elements having $\mathrm{b}^{\leq}$-index n as follows:

$$(\downarrow_{n+1} u) \;=\; \bigcap_{p \in dom(u),\, v \not\sim_n u_p} ((\downarrow_n v) \to \bigcup_{v \not\leq_n w} (\downarrow_n w)). \tag{10}$$

Notice that all intersections and unions involved in the above formula are finite. Indeed, we have already observed that there are only finitely many elements of the kind $\downarrow_n w$. Moreover, if $v_1 \sim_n v_2$, then $\downarrow_n v_1 = \downarrow_n v_2$ and also $v_1 \leq_n w$ if and only if $v_2 \leq_n w$, see Lemma 6. As a consequence, $(\downarrow_n v_1) \to \bigcup_{v_1 \not\leq_n w} (\downarrow_n w)$ equals $(\downarrow_n v_2) \to \bigcup_{v_2 \not\leq_n w} (\downarrow_n w)$.

Let us verify equation (10). Suppose that $z \leq_{n+1} u$ and let $v : Q \longrightarrow L$ be arbitrary with the property that $v \not\sim_n u_p$, for every point p in the domain of u. We show that $z \in (\downarrow_n v) \to \bigcup_{\{w \mid v \not\leq_n w\}} (\downarrow_n w)$ using (9). Let q be a point in the domain of z such that $z_q \leq_n v$. From $z \leq_{n+1} u$, we conclude that there exists p such that $z_q \sim_n u_p$. Consequently, $v \not\leq_n z_q$, otherwise $z_q \sim_n v$ and

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

so $v \sim_n u_p$, contradicting the choice of v. Therefore, $z_q \in \downarrow_n z_q \subseteq \bigcup_{v \not\leq_n w} (\downarrow_n w)$. Vice versa, suppose that $z \not\leq_{n+1} u$. It follows that there is a point q in the domain of z such, that for every point p in the domain of u, $z_q \not\sim_n u_p$. We check that $z \notin (\downarrow_n z_q) \longrightarrow \bigcup_{z_q \not\leq_n w} \downarrow_n (w)$. This is clear as $z_q \in (\downarrow_n z_q)$ and $z_q \notin \bigcup_{z_q \not\leq_n w} (\downarrow_n w)$.

This proves equation (10) and ends the proof of the Lemma. □

The following statement is an immediate consequence of the finite model property:

Lemma 12. *Every finitely presented Heyting algebra embeds into a product of finite Heyting algebras.*

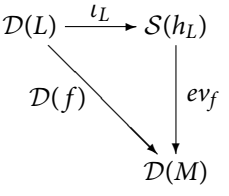
Recall that, by Birkhoff duality, monotone maps $f : M \longrightarrow L$ between finite posets M, L bijectively (and naturally) correspond to bound-preserving lattice homomorphism $f^{-1} = \mathcal{D}(f) : \mathcal{D}(L) \to \mathcal{D}(M)$. Therefore, for $f : M \longrightarrow L$, we define a map

$$ev_f : \mathcal{S}(h_L) \longrightarrow \mathcal{D}(M)$$

by putting, for $X \in \mathcal{S}(h_L)$,

$$ev_f(X) := \{\, p \in M \mid f_p \in X_{\downarrow p} \,\}. \tag{11}$$

Proposition 13. *The map ev_f is a Heyting algebra morphism and makes the following diagram commute:*



Consequently, $\mathcal{S}(h_L)$, together with ι_L as the canonical embedding, is a free Heyting algebra generated by the finite distributive lattice $\mathcal{D}(L)$.

Proof. Let us verify first that the above diagram commutes. For each $d \in \mathcal{D}(L)$,

$$\begin{aligned} ev_f(i_L(d)) &= \{\, p \in M \mid f_p \in i_L(d)_{\downarrow p} \,\} \\ &= \{\, p \in M \mid f_p(p) \in d \,\} \\ &= \{\, p \in M \mid f(p) \in d \,\} = \mathcal{D}(f)(d). \end{aligned}$$

To see that ev_f is a Heyting algebra homomorphism, we have, e.g.

$$\begin{aligned} ev_f(S \to T) &= \{\, p \in M \mid f_p \in (S \to T)_{\downarrow p} \,\} \\ &= \{\, p \in M \mid \forall q \in\downarrow p\, (f_{pq} \in S_{\downarrow q} \Rightarrow f_{pq} \in T_{\downarrow q}) \,\} \\ &= \{\, p \in M \mid \forall q \leq p\, (f_q \in S_{\downarrow q} \Rightarrow f_q \in T_{\downarrow q}) \,\} \\ &= ev_f(S) \to ev_f(T). \end{aligned}$$

Notice also that, in view of Lemma 11, ev_f is the unique Heyting algebra morphism $g : \mathcal{S}(h_L) \to \mathcal{D}(M)$ with the property that $g \circ i_L = \mathcal{D}(f)$. Therefore, we have argued that every bounded lattice morphism $g = \mathcal{D}(f) : \mathcal{D}(L) \longrightarrow \mathcal{D}(M)$, where M is a finite poset, extends uniquely to the Heyting algebra morphism $ev_f : \mathcal{S}(h_L) \longrightarrow \mathcal{D}(M)$. By a standard argument, the same universal property

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

holds with respect to the bound-preserving lattice homomorphisms $g : \mathcal{D}(L) \longrightarrow H$, where now H is a sub-Heyting algebra of a product of finite Heyting algebras of the form $\mathcal{D}(M)$. In particular, using Lemma 12, we can take (g, H) to be (η, F), the free Heyting algebra generated by the distributive lattice $\mathcal{D}(M)$. Then, by combining the universal properties of $(\iota_L, \mathcal{S}(h_L))$ and of (η, F), it follows that $\mathcal{S}(h_L)$ and F are isomorphic. □

Let **HD** be the category of Heyting algebras freely generated by a finite distributive lattice and let $\mathbf{M_H}$ be the subcategory of presheaves over $\mathbf{P_0}$ having as objects the evaluations sheaves and as arrows the natural transformations having a b-index. We want to show that **HD** is dual to $\mathbf{M_H}$.

We define the following functor $\mathbf{T_H}$:

$$\begin{array}{ccc} \mathbf{M_H} & \xrightarrow{\quad \mathbf{T_H} \quad} & \mathbf{HD}^{op} \\ \\ h_L & & \mathcal{S}(h_L) \\ \Big\downarrow f & \longmapsto & \Big\uparrow f^{-1}=\mathbf{T_H}(f) \\ h_M & & \mathcal{S}(h_M) \end{array}$$

where $\mathcal{S}(h_M)$ is as in Lemma 11 and f^{-1} is the inverse image function.

Lemma 14.

(i) $\mathbf{T_H}$ *is a well-defined functor.*

(ii) $\mathbf{T_H}$ *is essentially surjective.*

Proof. By Proposition 13, $\mathcal{S}(h_L)$ is a Heyting algebra freely generated by a finite distributive lattice and every such Heyting algebra is isomorphic to one of that form. Hence, $\mathbf{T_H}$ is well defined on objects and essentially surjective. Clearly, $\mathbf{T_H}$ preserves compositions and identities. We need to show that for any subpresheaf D of h_M with a b-index, $f^{-1}(D)$ has a b-index and that f^{-1} is a Heyting algebra morphism. The latter follows from the fact that $f^{-1} : Sub(h_M) \longrightarrow Sub(h_L)$ is a Heyting algebra morphism and that $\mathcal{S}(h_L)$, $\mathcal{S}(h_M)$ are sub-Heyting algebras of the Heyting algebras of subpresheaves $Sub(h_L)$, $Sub(h_M)$, respectively.

Let n be a b-index of D and m a b-index of f. We shall show that $f^{-1}(D)$ has b-index $n + m$. Let $v \in f^{-1}(D)$ and v' be such that $v \sim_{n+m} v'$. By Proposition 2, $f(v) \sim_n f(v')$. Since $f(v) \in D$ and D is $\sim_n$-closed, it follows that $f(v') \in D$ and then $v' \in f^{-1}(D)$. □

Recall from Proposition 13 that, for $u : P \longrightarrow L$, ev_u is the unique Heyting algebra morphism $\mathcal{S}(h_L) \longrightarrow \mathcal{D}(P)$ such that $\mathcal{D}(u) = ev_u \circ \iota_L$. Conversely, given a Heyting algebra morphism $\alpha : \mathcal{S}(h_L) \longrightarrow \mathcal{D}(P)$, we define an L-evaluation

$$\overline{\alpha} : P \longrightarrow L$$

as the dual of the distributive lattice morphism $\alpha \circ \iota_L$. By the definition of $\overline{\alpha}$, the diagram

$$\begin{array}{ccc} \mathcal{D}(L) & \xrightarrow{\iota_L} & \mathcal{S}(h_L) \\ & \searrow^{\mathcal{D}(\overline{\alpha})} & \Big\downarrow \alpha \\ & & \mathcal{D}(L) \end{array}$$

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

commutes and therefore, by the universal property of ev, we deduce the following relation:

$$ev_{\overline{\alpha}} = \alpha\,. \tag{12}$$

The two maps

$$\alpha \mapsto \overline{\alpha} \qquad u \mapsto ev_u$$

yield a bijective correspondence between the Heyting algebra morphisms $\alpha : \mathcal{S}(h_L) \longrightarrow \mathcal{D}(P)$ and the L-evaluations $u \in h_L(P)$ which is natural in P. This immediately follows from the chain of natural isomorphisms

$$\mathbf{POS}(P, L) \simeq \mathbf{DLATT}(\mathcal{D}(L), \mathcal{D}(P)) \simeq \mathbf{HA}(\mathcal{S}(h_L), \mathcal{D}(P)),$$

where the first natural isomorphism is Birkhoff duality between the category of finite posets and the category of finite distributive lattices, and the second is by freeness of $\mathcal{S}(h_L)$, Proposition 13.

Let h_L, h_M be objects of $\mathbf{HD}$, $\mu : \mathcal{S}(h_L) \longrightarrow \mathcal{S}(h_M)$ be a morphism of Heyting algebras. For each $P \in \mathbf{P_0}$, we define

$$\mu^*_P :\ h_M(P) \longrightarrow h_L(P)$$

as follows:

$$\mu^*_P(u) := \overline{ev_u \circ \mu}\,, \qquad \text{for each } u \in h_M(P).$$

Note that by the above correspondence, it is immediate that $\mu^*_P(u) \in h_L(P)$ and that $\mu^* : h_M \longrightarrow h_L$ is a natural transformation. Moreover,

Proposition 15. *With the notation as above, we have*

(i) $\mu^*_P(u) \in X_P$ *iff* $u \in \mu(X)_P$, *for* $X \in \mathcal{S}(h_L)$ *and* $u \in h_M(P)$;
(ii) $\mu^* : h_M \longrightarrow h_L$ *is a morphism in* $\mathbf{M_H}$;
(iii) $\mu = (\mu^*)^{-1} = \mathbf{T_H}(\mu^*)$;
(iv) $f = (f^{-1})^*$, *for any morphism* $f : h_M \longrightarrow h_L$ *in* $\mathbf{M_H}$.

Proof. Ad (i). Observe that, for any $v \in h_M(Q)$ and $Y \in \mathcal{S}(h_L)$, $ev_v(Y) = Q$ iff, for all $q \in Q$, $v_q \in Y_{\downarrow q}$, iff $v_{\rho(Q)} \in Y_{\downarrow \rho(Q)}$ iff $v \in Y_Q$. Recall now – see equation (12) – that, for any $\alpha : \mathcal{S}(h_L) \longrightarrow \mathcal{D}(M)$, $ev_{\overline{\alpha}} = \alpha$ and so, in particular, $ev_{\mu^*_P(u)} = ev_{\overline{ev_u \circ \mu}} = ev_u \circ \mu$. Therefore, for $X \in \mathcal{S}(h_L)$ and $u : P \longrightarrow M$, we have $ev_{\mu^*_P(u)}(X) = ev_u(\mu(X))$ and therefore, according to the previous observation, we have $\mu^*_P(u) \in X$ iff $ev_{\mu^*_P(u)}(X) = P$ iff $ev_u(\mu(X)) = P$ iff $u \in \mu(X)_P$.

Ad (ii). We need to show that the transformation μ^* has a b-index. Let $n \in \omega$ be the maximum of the b-indexes of sets of $\mu(X)$ where X is of the kind $\iota_L(d)$ for some $d \in \mathcal{D}(L)$. Notice that there are only finitely many such X's and, moreover, for $w, w' \in h_L$ we have $w \sim_0 w'$ iff w, w' belong to the same such X's. For any $u \in h_M(P)$ and $v \in h_M(Q)$ such that $u \sim_n v$ and for $X = \iota_L(d)$, we have

$$\dfrac{\dfrac{\dfrac{\mu^*_Q(v) \in X_Q}{v \in \mu(X)_Q}}{u \in \mu(X)_P}}{\mu^*_P(u) \in X_P} \quad \text{by (i)}$$

where the horizontal lines above stand for logical equivalences. Thus, $\mu^*_Q(v) \sim_0 \mu^*_P(u)$ and μ^* has b-index n.

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

Ad (iii). Using (i), we have, for any $X \in \mathcal{S}(h_L)$ and $v \in h_M(P)$,

$$\frac{\dfrac{v \in (\mu_P^*)^{-1}(X)}{\mu_P^*(v) \in X}}{v \in \mu(X)_P}$$

i.e. $\mu = (\mu^*)^{-1}$.

Ad (iv). Let $v \in h_M(P)$, $p \in P$ and $d \in \mathcal{D}(L)$. Then, we have

$$\frac{\dfrac{\dfrac{\dfrac{\dfrac{(f^{-1})_P^*(v)(p) \in d}{(f^{-1})_{\downarrow p}^*(v_p) \in \iota_L(d)_{\downarrow p}}}{v_p \in (f^{-1}(\iota_L(d)))_{\downarrow p}}}{f_{\downarrow p}(v_p) \in \iota_L(d)_{\downarrow p}}}{f_P(v)(p) \in d}$$

by the definition of ι_L,

using (i),

Since P, v, p, and d were arbitrary $f = (f^{-1})^*$. □

Thus, we have

Theorem 16. (Duality Theorem). *The functor* $\mathbf{T_H} : \mathbf{M_H} \longrightarrow \mathbf{HD}^{op}$ *is an equivalence of categories.*

Proof. Lemma 14 shows that $\mathbf{T_H}$ is a functor which is essentially surjective and by Lemma 15(ii)–(iv) $\mathbf{T_H}$ is full and faithful, i.e. $\mathbf{T_H}$ is an equivalence of categories. □

For some applications in Section 9, we shall need a duality theorem for some subvarieties. Call a variety $\mathbf{V}$ of Heyting algebras *finitely approximable*, if every finitely generated free $\mathbf{V}$-algebra embeds into a product of finite $\mathbf{V}$-algebras.

We can extend the above Duality Theorem to finitely approximable subvarieties as follows. Take one such subvariety $\mathbf{V}$ and let $\mathbf{P_0^V}$ be the category of finite rooted posets P such that $\mathcal{D}(P) \in \mathbf{V}$. Let $\mathbf{HD^V}$ be the category of $\mathbf{V}$-algebras freely generated by a finite distributive lattice and let $\mathbf{M_H^V}$ be the subcategory of presheaves over $\mathbf{P_0^V}$ having as objects the evaluations sheaves and as arrows the natural transformations having a b-index. We have

Theorem 17. (Duality Theorem for Finitely Approximable Subvarieties). *For every finitely approximable variety* $\mathbf{V}$ *of Heyting algebras,* $\mathbf{HD^V}$ *is dual to* $\mathbf{M_H^V}$.

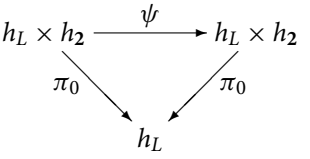
Proof. By reading back the proof of Theorem 16, it is immediately realized that Lemma 12 is the only specific fact on Heyting algebras we used. When this Lemma is replaced by the assumption that $\mathbf{V}$ is finitely approximable, the same chain of arguments yields a proof of Theorem 17. □

5. Indexes and Periods Over Finite Models

Taking into consideration the algebraic reformulation from Section 2 and the information from Section 4, we can prove Ruitenburg's Theorem for (*IPC*) by showing that *all natural transformations from* $h_L \times h_{\mathbf{2}}$ *into itself, commuting over the first projection* π_0 *and having a b-index, are*

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

ultimately periodic with period 2. Spelling this out, this means the following. Fix a finite poset L and a natural transformation $\psi : h_L \times h_{\mathbf{2}} \longrightarrow h_L \times h_{\mathbf{2}}$ having a b-index such that the diagram



commutes; we have to find an N such that $\psi^{N+2} = \psi^N$, according to the dual reformulation of (2).

From the commutativity of the above triangle, we can decompose ψ as $\psi = \langle \pi_0, \chi \rangle$, were both $\pi_0 : h_L \times h_{\mathbf{2}} \longrightarrow h_L$ and $\chi : h_L \times h_{\mathbf{2}} \longrightarrow h_{\mathbf{2}}$ have a b-index (actually, π_0 has b-index 0, being a projection); we assume that $n \geq 1$ is a b-index for both of them. *We let such $\psi = \langle \pi_0, \chi \rangle$ and n be fixed for the remaining part of this and next two sections.*

Notice that for $(v, u) \in h_L(P) \times h_{\mathbf{2}}(P)$, we have

$$\psi^k(v, u) = (v, u_k),$$

where we put

$$u_0 := u \text{ and } u_{k+1} := \chi(v, u_k). \tag{13}$$

Since P and L are finite, it is clear that the sequence $\{ \psi^k(v, u) \mid k \geq 0 \}$ (and obviously also the sequence $\{ u_k \mid k \geq 0 \}$) must become ultimately periodic.

We show in this section that, for each finite poset P and for each $(v, u) \in h_L(P) \times h_{\mathbf{2}}(P)$, the period of the sequence $\{ \psi^k(v, u) \mid k \geq 0 \}$ has 2 as an upper bound, whereas the index of $\{ \psi^k(v, u) \mid k \geq 0 \}$ can be bounded by the maximum length of the chains in the finite poset P. In the next section, we shall bound such an index independently of P, thus proving Ruitenburg's Theorem.

Call $(v, u) \in h_L(P) \times h_{\mathbf{2}}(P)$ *2-periodic* (or just *periodic*[4]) if $\psi^2(v, u) = (v, u)$; a point $q \in P$ is similarly said periodic in (v, u) iff $(v, u)_q$ is periodic. We shall only say that p is periodic if an evaluation is given and understood from the context. We call a point *non-periodic* if it is not periodic (w.r.t. a given evaluation).

Lemma 18. *Let $(v, u) \in h_L(P) \times h_{\mathbf{2}}(P)$ and $p \in P$ be such that all $q \in P$, $q < p$, are periodic. Then either $(v, u)_p$ is periodic or $\psi(v, u)_p$ is periodic. Moreover, if $(v, u)_p$ is non-periodic and $u_0(p) = u(p) = 1$, then $u_1(p) = \chi(u, v)(p) = 0$.*

Proof. Let $\Downarrow p := \{ q \in P \mid q < p \}$. We shall represent $(u_k)_p$ as a pair (a_k, x_k), where $a_k = u_k(p)$ and x_k is the restriction of $(u_k)_p$ to $\Downarrow p$. Notice that, by assumption, $x_{k+2} = x_k$, for $k \geq 0$. To emphasize that (a_k, x_k) represents a colored poset, we use the notation $\begin{array}{c} a_k \\ \diagup \quad \diagdown \\ x_k \end{array}$ for this pair.

Let us start by considering a first repeat (i, j) of the sequence $\{ a_k \}_{k \geq 0}$ – i.e. $i \geq 0$ is the smallest i such that there is $j > 0$ such that $a_{i+j} = a_i$ and j is the smallest such j. Since the a_n can only take value 0 or 1, we must have $i + j \leq 2$. We show that the sequence $\{ (u_k)_p \}_{k \geq 0}$ has first repeat taken from

$$(0, 1), (0, 2), (1, 1), (1, 2)\,.$$

This shall imply in the first two cases that $(v, u)_p$ is periodic or, in the last two cases, that $\psi(v, u)_p$ is periodic. To our goal, let $x = x_0$, $y = x_1$, and recall that we do now know whether $x = y$.

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

Notice that, if $j = 2$, then $i = 0$ and a first repeat for $\{ (u_k)_p \}_{k \geq 0}$, is $(0, 2)$, as in the diagram below

$$\begin{array}{ccc} a & b & a \\ x & y & x \end{array}$$

Therefore, let us assume $j = 1$, so $i \in \{ 0, 1 \}$. Consider firstly $i = 0$:

$$\begin{array}{cccc} a & a & c & d \\ x & y & x & y \end{array}$$

If $x = y$, then we have a repeat at $(0, 1)$. Also, if $a = 1$, then the mappings x and y are uniformly 1 (since evaluations are order-preserving maps and we have $1 \leq 0$ in $\mathbf{2}$): again, $x = y$ and $(0, 1)$ is a repeat.

So let us assume $x \neq y$ and $a = 0$. If $c = a$, then we have the repeat $(0, 2)$ as above. Otherwise, $c = 1$, so $x = 1$. We cannot have $d = 1$, otherwise $1 = x = y$. Thus, $d = 0 = a$, and the repeat is $(1, 2)$.

Finally, consider $i = 1$ (so $a \neq b$ and $j = 1$):

$$\begin{array}{cccc} a & b & b & d \\ x & y & x & y \end{array}$$

We have two subcases: $b = 1$ and $b = 0$. If $b = 1$, then $a = 0$ and $x = 1 = y$: we have a repeat at $(1, 1)$.

In the last subcase, we have $b = 0$, $a = 1$ and now if $d = 0$ we have a repeat at $(1, 2)$ and if $d = 1$ we have a repeat $(1, 1)$ (because $d = a = 1$ implies $y = 1$ and $x = 1$).

The last statement of the lemma is also obvious in view of the fact that if $a = b = 1$, then $x = y = 1$, so p is periodic. □

Corollary 19. *Let N_P be the height of P, then $\psi^{N_P}(v, u)$ is periodic for all $(v, u) \in h_L(P) \times h_{\mathbf{2}}(P)$.*

Proof. An easy induction on N_P, based on the previous Lemma. □

6. Ranks

Ranks, already introduced in Fine (1985), are a powerful tool that goes hand in hand with bounded bisimulations; in our context, the useful notion of rank is given below. Recall that $\psi = \langle \pi_0, \chi \rangle$ and that $n \geq 1$ is a b-index for ψ and χ.

Let $(v, u) \in h_L(P) \times h_{\mathbf{2}}(P)$ be given. The *type* of a periodic point $p \in P$ is the pair of equivalence classes

$$\langle [(v_p, u_p)]_{n-1}, [\psi(v_p, u_p)]_{n-1} \rangle. \tag{14}$$

The *rank* of a point p (that we shall denote by $rk(p)$) is the cardinality of the set of distinct types of the periodic points $q \leq p$. Since $\sim_{n-1}$ is an equivalence relation with finitely many equivalence classes, the rank cannot exceed a positive number $R(L, n)$ (that can be computed in function of L, n).

Clearly, we have $rk(p) \geq rk(q)$ in case $p \geq q$. Notice that an application of ψ does not decrease the rank of a point: this is because the pairs (14) coming from a periodic point just get swapped after applying ψ. A nonperiodic point $p \in P$ has *minimal rank* iff we have $rk(p) = rk(q)$ for all non-periodic $q \leq p$.

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

Lemma 20. *Let $p \in P$ be a non-periodic point of minimal rank in $(v,u) \in h_L(P) \times h_2(P)$; suppose also that (v,u) is constant on the set of all non-periodic points in $\downarrow p$. Then we have $\psi^m(v,u)_{q_0} \sim_n \psi^m(v,u)_{q_1}$ for all $m \geq 0$ and for all non-periodic points $q_0, q_1 \leq p$.*

Proof. We let Π be the set of periodic points of (v,u) that are in $\downarrow p$ and let Π^c be $(\downarrow p) \setminus \Pi$. Let us first observe that for every $r \in \Pi^c$, we have

$$\begin{aligned}\{\langle [(v_s,u_s)]_{n-1}, [\psi(v_s,u_s)]_{n-1}\rangle \mid s \leq r,\ s \text{ is periodic}\}\\ = \{\langle [(v_s,u_s)]_{n-1}, [\psi(v_s,u_s)]_{n-1}\rangle \mid s \leq p,\ s \text{ is periodic}\}\end{aligned}$$

(indeed the inclusion $\subseteq$ is because $r \leq p$ and the inclusion $\supseteq$ is by the minimality of the rank of p). Saying this in words, we have that "for every periodic $s \leq p$ there is a periodic $s' \leq r$ such that $(v_s,u_s) \sim_{n-1} (v_{s'},u_{s'})$ and $\psi(v_s,u_s) \sim_{n-1} \psi(v_{s'},u_{s'})$"; also (by the definition of 2-periodicity), "for all $m \geq 0$, for every periodic $s \leq p$ there is a periodic $s' \leq r$ such that $\psi^m(v_s,u_s) \sim_{n-1} \psi^m(v_{s'},u_{s'})$." By letting both q_0, q_1 playing the role of r, we get

Fact. For every $m \geq 0$, for every $q_0, q_1 \in \Pi^c$, for every periodic $s \leq q_0$ there is a periodic $s' \leq q_0$ such that $\psi^m(v_s,u_s) \sim_{n-1} \psi^m(v_{s'},u_{s'})$ (and vice versa).

We now prove the statement of the lemma by induction on m; take two points $q_0, q_1 \in \Pi^c$.

For $m = 0$, $(v,u)_{q_0} \sim_n (v,u)_{q_1}$ is established as follows: as long as Player 1 plays in Π^c, we know (v,u) is constant so that Player 2 can answer with an identical move still staying within Π^c; as soon as he plays in Π, Player 2 uses the above Fact to win the game.

The inductive case $\psi^{m+1}(v,u)_{q_0} \sim_n \psi^{m+1}(v,u)_{q_1}$ is proved in the same way, using the Fact (which holds for the integer $m+1$) and observing that ψ^{m+1} is constant on Π^c. The latter statement can be verified as follows: by the induction hypothesis we have $\psi^m(v,u)_q \sim_n \psi^m(v,u)_{q'}$, so we derive from Proposition 2 $\psi^{m+1}(v,u)_q \sim_0 \psi^{m+1}(v,u)_{q'}$, for all $q, q' \in \Pi^c$, i.e. ψ^{m+1} is constant on Π^c. □

7. Ruitenburg's Theorem

We can finally prove:

Theorem 21. (Ruitenburg's Theorem for IPC). *There is $N \geq 1$ such that we have $\psi^{N+2} = \psi^N$.*

Proof. Let L be a finite poset and let $R := R(L,n)$ be the maximum rank for n, L (see the previous section). Below, for $e \in L$, we let $|e|$ be the height of e in L, i.e. the maximum size of chains in L whose maximum element is e; we let also $|L|$ be the maximum size of a chain in L. We make an induction on natural numbers $l \geq 1$ and show the following: for each $l \geq 1$, there is $N(l)$ such that, for every (v,u) and $p \in dom(v,u)$ with $l \geq |v(p)|$, $\psi^{N(l)}(v_p,u_p)$ is periodic. It will turn out that $N(l)$ is $2R(l-1)+1$. Once this is proved, the statement of the theorem shall be proved with $N = N(|L|)$.

If $l = 1$, it is easily seen that we can put $N(l) = 1$ (this case is essentially the classical logic case).

Pick a p with $|v(p)| = l > 1$; let N_0 be the maximum of the values $N(l_0)$ for $l_0 < l$:[5] we show that we can take $N(l)$ to be $N_0 + 2R$.

Firstly, let $(v,u_0) := \psi^{N_0}(v,u)$ so all q with $|v(q)| < l$ are periodic in (v,u_0). After such iterations, suppose that p is not yet periodic in (v,u_0). We let r be the minimum rank of points $q \leq p$ which are not periodic (all such points q must be such that $v(q) = v(p)$).

We show that after *two iterations* of ψ, all points $p_0 \leq p$ having rank r become periodic or increase their rank, thus causing the overall minimum rank below p to increase. This implies that after at most $2(R-r) \leq 2R$ iterations of ψ, all points below p, p itself included, become periodic. Otherwise said, we take $R - r$ as the secondary parameter of our double induction.

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

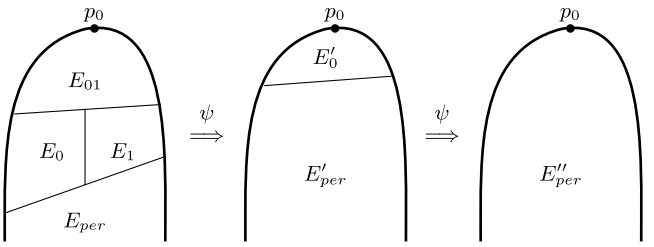


Figure 1. Iterating twice ψ to make p_0 periodic.

Pick $p_0 \leq p$ having minimal rank r; thus, we have that all $q \leq p_0$ in (v, u_0) are now either periodic or have the same rank and the same v-value as p_0 (by the choice of N_0 above). Let us divide the points of $\downarrow p_0$ into four subsets:

$$\begin{aligned}
E_{per} &:= \{\, q \mid\ q \text{ is periodic} \,\} \\
E_0 &:= \{\, q \mid\ q \notin E_{per} \;\&\; \forall q' \leq q\, (q' \notin E_{per} \Rightarrow u_0(q') = 0) \,\} \\
E_1 &:= \{\, q \mid\ q \notin E_{per} \;\&\; \forall q' \leq q\, (q' \notin E_{per} \Rightarrow u_0(q') = 1) \,\} \\
E_{01} &:= \{\, q \mid\ q' \notin E_{per} \cup E_1 \cup E_0 \,\}.
\end{aligned}$$

Let us define a *frontier point* to be a non-periodic point $f \leq p$ such that all $q < f$ are periodic. Clearly, a frontier point f belongs to $E_0 \cup E_1$, since f itself is the only nonperiodic $q' \leq f$. By Lemma 18, all frontier points become periodic after applying ψ. Take a point $q \in E_i$ and a frontier point f below it; since q also has minimal rank and the hypotheses of Lemma 20 are satisfied for $(v, u)_q$, we have in particular that $\psi^m(v, u_0)_{q'} = \psi^m(v, u_0)_f$ for all $m \geq 0$ and all non-periodic $q' \leq q$, and hence $\psi(v, u_0)_q$ is periodic too.

Thus, if we apply ψ, we have that in $(v, u_1) := \psi(v, u_0)$ all points in $E_{per} \cup E_0 \cup E_1$ become periodic, together with possibly some points in E_{01}. The latter points get in any case u_1-value equal to 0. This can be seen as follows. If any such point gets u_1-value equal to 1, then all points below it get the same u_1-value. Yet, by definition, these points are above some frontier point in E_1 and frontier points in E_1 get u_1-value 0 by the second statement of Lemma 18.

If $p_0 \in E_0$ has become periodic, we are done; we are also done if the rank of p_0 increases, because this is precisely what we want. If p_0 has not become periodic and its rank has not increased, then now all the non-periodic points below p_0 in (v, u_1) have u_1-value 0 (by the previous remark) and have the same rank as p_0. Thus, they are the set E_0 computed in (v, u_1) (instead of in (v, u_0)) and we know by the same considerations as above that it is sufficient to apply ψ once more to make them periodic. □

Figure 1 illustrates the main step of the proof, the double iteration of ψ to turn p_0 into a periodic point. Notice that some crucial arguments used in the above proof, starting from the induction on $|e|$ itself, make essential use of the fact that evaluations are order-preserving, so such arguments are not suitable for modal logics.

8. A Non-ultimately Periodic Endomorphism

Ruitenburg's Theorem, interpreted over finitely generated free Heyting algebras, says that any endomorphism of such algebras

$$\mu : \mathcal{F}_H(x_1, \ldots, x_n) \longrightarrow \mathcal{F}_H(x_1, \ldots, x_n)$$

is ultimately periodic with period 2, in case it fixes all free generators but one. One may ask whether this is a peculiar property of the endomorphisms fixing all free generators but one or

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

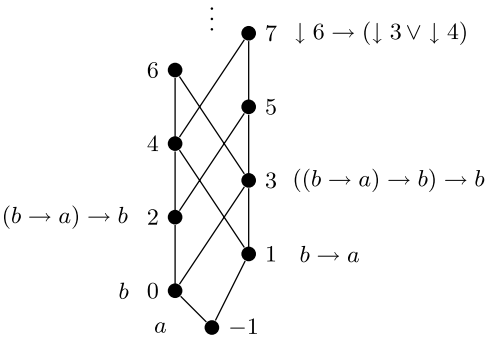


Figure 2. The modified Rieger–Nishimura ladder.

whether this can be extended to all endomorphism: we show by a counterexample that there exist endomorphisms of the free algebra over *two* generators which are not periodic.

To describe our counterexample, we first introduce a variant $(R, \leq)$ of the Rieger–Nishimura ladder. This is the poset so described:

- $R = \{n \in \mathbb{Z} \mid n \geq -1\}$;
- $n \leq m$ iff either $n = -1$ or ($n \geq 0$ and either $n \leq m - 2$ or $n = m$).

It is not difficult to see that $\leq$ is a reflexive, transitive, antisymmetric relation (actually, $(R, \leq)$ differs from Rieger–Nishimura only for the presence of the bottom element -1, see Figure 2).

Let us consider the Heyting algebra $\mathcal{D}(R)$ of downsets of $(R, \leq)$. We show that this is generated by the two downsets $a = \{-1\}$ and $b = \{0, -1\}$. To see this, we show that, for all $n \in R$, the downset $\downarrow n$ belongs to the subalgebra generated by a, b. In fact, we have that:

- $\downarrow -1 = a$;
- $\downarrow 0 = b$;
- $\downarrow 1 = b \to a$;
- $\downarrow 2 = (b \to a) \to b$;
- $\downarrow 3 = ((b \to a) \to b) \to b$;
- $\downarrow n + 4 = \downarrow (n + 3) \to \downarrow n \vee \downarrow (n + 1)$, for $n \geq 0$.

Remark 22. Let $d \in \mathcal{D}(R)$ be such that $d \neq \emptyset$ and $d \neq R$. Then either $d = \downarrow n$, for some $n \geq -1$, or d has two maximal elements n and $n + 1$, so $d = \downarrow n \cup \downarrow (n + 1)$. In the latter case, both $n + 3$ and $n + 4$ are upper bounds of d, but $n + 3$ is such that $\mathrm{card}(\downarrow (n + 3)) = \mathrm{card}(d) + 1$, while $\mathrm{card}(\downarrow (n + 4)) = \mathrm{card}(d) + 2$. We let therefore:

$$\bigvee(\downarrow n) := n, \qquad \bigvee(\downarrow n \cup \downarrow (n + 1)) := n + 3.$$

Lemma 23. *Let F be the free Heyting algebra over two generators a, b divided by the congruence generated by*

$$\top = \neg\neg a \wedge (a \to b). \tag{15}$$

The Heyting algebra $\mathcal{D}(R)$ is isomorphic to F.

Proof. Since, within $\mathcal{D}(R)$, the downset $\{-1\}$ is a least nontrivial element (so $\neg\{-1\} = \emptyset$) and $\{-1\} \subseteq \{0, -1\}$, it is clear that $\mathcal{D}(R)$ satisfies the equality (15) for $a := \{-1\}$ and $b := \{0, -1\}$. Also, $\mathcal{D}(R)$ is generated by the two elements $\{0, -1\}$ and $\{-1\}$; as a consequence, the function $q : F \longrightarrow \mathcal{D}(R)$ mapping the equivalence class of the free generator b to $\{0, -1\}$ and the equivalence class of the free generator a to $\{-1\}$ is a Heyting algebras quotient. To show that this quotient map is also injective, we use the same technique we adopted for showing that $\mathcal{S}(h_L)$ is the free algebra over the

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

distributive lattice $\mathcal{D}(L)$: since F embeds into a product of finite Heyting algebras (like any finitely presented Heyting algebra, see Lemma 12), it is sufficient to show that any morphism $h : F \longrightarrow \mathcal{D}(P)$, for a finite poset $(P, \leq)$, factors through q. This follows from the following statement on finite Kripke models:

(*) for every finite Kripke model over P validating $\neg\neg a \wedge (a \to b)$, there is an open map $f : (P, \leq) \longrightarrow (R, \leq)$ preserving the evaluation of a, b.

Property (*) is easily checked by defining $f(p)$, for $p \in P$, by induction on the height of p. In detail:

(i) $f(p) := -1$ if p forces both a, b;
(ii) $f(p) := 0$ if p forces only b;

If p forces neither a nor b, then

(iii) if all $p' < p$ force both a and b, then $f(p) := 1$;
(iv) if all $p' < p$ force b and there is $p' < p$ forcing only b, then $f(p) := 2$;
(v) in all remaining cases, $f(p) := \bigvee\!\!\bigvee \{ f(p') \mid p' < p \}$.

Notice that the above analysis is exhaustive: since $a \to b$ is true everywhere, there cannot be points forcing only a and not b. Similarly, since $\neg\neg a$ is true everywhere, for every p there must be $p' \leq p$ forcing a: this fact is used when checking that f as defined above is open. □

Remark 24. Alternatively, Lemma 23 can be proved by observing that R is the set of points in the canonical/universal model on the variables a and b which make the formula $\neg\neg a \wedge (a \to b)$ true (we thank an anonymous referee for this observation). For background information on universal models, see Bellissima (1986).

Lemma 25. *There is an endomorphism of $\mathcal{D}(R)$ which is not ultimately periodic.*

Proof. The endomorphism is the inverse image f^{-1} along the open map $f : (R, \leq) \longrightarrow (R, \leq)$ so defined:

$$f(n) := -1\,, \text{ for } n < 2\,, \qquad f(n) := n - 2\,, \text{ for } n \geq 2\,.$$

It is evident that f^{-1} is not ultimately periodic: this comes from the fact that we have $f(n) = n - 2$ for all $n \geq 2$. □

To lift the endomorphism of Lemma 25 to the level of the free algebra on two generators, we first show that $\mathcal{D}(R)$ is a projective algebra:

Lemma 26. *$\mathcal{D}(R)$ is a projective Heyting algebra.*

Proof. We might use for the proof of this Lemma the general results from Ghilardi (1999); however, we prefer to supply a direct proof. Let $F_H(a, b)$ be the free Heyting algebra on two generators and let $q : F_H(a, b) \longrightarrow \mathcal{D}(R)$ be the homomorphism mapping the free generator b to $\{0, -1\}$ and the free generator a to $\{-1\}$: what we have to produce is a section of q, namely a morphism s in the opposite direction such that $q \circ s = id$. Taking into consideration Lemma 23 and turning the existence of s into logical terms, what we need is a substitution σ such that the formulae

$$\sigma(\neg\neg a \wedge (a \to b))$$
$$\neg\neg a \wedge (a \to b) \to (a \leftrightarrow \sigma(a))$$
$$\neg\neg a \wedge (a \to b) \to (b \leftrightarrow \sigma(b))$$

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

are provable in intuitionistic logic (here $\sigma(a), \sigma(b)$ must be formulae over the propositional variables a, b). The required substitution in fact exists and can be taken to be

$$a \longmapsto \neg\neg a \to a, \qquad b \longmapsto ((\neg\neg a \to a) \to b) \to b$$

as it can be easily checked. □

Theorem 27. *There is an endomorphism of the free Heyting algebra on two generators which is not ultimately periodic.*

Proof. Let $f : \mathcal{D}(R) \longrightarrow \mathcal{D}(R)$ be the morphism defined in Lemma 25, so $f^{i+p} \neq f^i$ for no $i \geq 0$ and $p \geq 1$. Let $q : F_H(a, b) \longrightarrow \mathcal{D}(R)$ and $s : \mathcal{D}(R) \longrightarrow F_H(a, b)$ as in the proof of Lemma 26, so $q \circ s = id$. Let $g := s \circ f \circ q$ and suppose that $g^{i+p} = g^i$. Then $s \circ f^{i+p} \circ q = s \circ f^i \circ q$ and, by precomposing with s and postcomposing with q, $f^{i+p} = f^i$, contradiction. □

9. Bounds for Periods

Theorem 27 shows that Ruitenburg's Theorem cannot be generalized to many variables substitutions. Yet, there are many substitutions whose associated endomorphisms are ultimately periodic: in particular, if we take into considerations subvarieties, it is clear that in a locally finite subvariety of Heyting algebras, all free algebra endomorphisms are ultimately periodic. So, a natural question arises: *what can we say about the index and the period of the free algebra endomorphisms which happen to be ultimately periodic?* Finding bounds for index and period (depending on the subvariety under consideration and on the number of the free generators) is a rather natural and challenging question from a mathematical point of view. It is analogous to problems largely investigated in the current literature on the modal μ-calculus (Afshari and Leigh, 2013; Czarnecki, 2010; Ghilardi et al. 2016, 2019; Gouveia and Santocanale, 2019; Milanese and Venema, 2019). Here, closure ordinals for fixpoint convergence of monotonic functions are studied, in the various classes of models. If a function is not monotonic but inflationary, one can still investigate closure ordinals of the inflationary fixpoints. If a function is not monotonic but still ultimately periodic, then the question bears on the index and the period, and on bounding them. We shall supply few initial results for this problem below.

We fix, in this section, a finite poset L and a natural transformation $\psi : h_L \longrightarrow h_L$. We shall pay a particular attention to the case where ψ is the dual of an endomorphism of a finitely generated free algebras. This happens exactly when ψ has a b-index and when L is of the form $\langle \mathcal{P}(\underline{x}), \supseteq \rangle$ for a finite set $\underline{x}$ (so $\mathcal{D}(L)$ is a free distributive lattice).

As we saw, ψ might not be ultimately periodic but, on the other hand, all components ψ_P of ψ are such (because the P are finite posets). We show that the period of ψ_P can be uniformly bounded depending on the sole cardinality of L (and not on the cardinality of P). More precisely, we have the following statement:

Proposition 28. *Let ℓ be the cardinality of L. For each finite set P and each $v \in h_L(P)$, the period of the sequence $\{ \psi_P^k(v) \mid k \geq 0 \}$ has $\ell!$ as an upper bound.*

The proposition is an immediate consequence of Lemma 29 below, for which we need to define a few concepts.

For a point $p \in P$, we let the *view set* of p (w.r.t. v, ψ) be the set $\{ \psi^k(v)(p) \mid k \geq 0 \}$ and, for $S \subseteq P$, we let the view set of S (w.r.t. v, ψ) be the union of the view sets of the $p \in S$.

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

Our claim follows from the following:

Lemma 29. *For $v \in h_L(P)$, the period of the sequence $\{ \psi^k(v) \mid k \geq 0 \}$ has as an upper bound $K!$, where K is the cardinality of the view set of P.*

Proof. We argue by induction on the height of P. If such an height is 1, then P contains only the root and the period is bounded by $K \leq K!$.

Suppose that the height of P is greater than 1 and let p be the root of P. Then, let $\Downarrow p := \{ q \in P \mid q < p \}$ and let M be the cardinality of the view set of $\Downarrow p$. By the induction hypothesis, for any $q \in \Downarrow p$, $M!$ is an upper bound for the period of the sequence $\{ \psi^k(v_q) \mid k \geq 0 \}$. Since the lcm of many copies of $M!$ is $M!$, the restriction of $\{ \psi^k(v) \mid k \geq 0 \}$ to $\Downarrow p$ has period $M!$.

Thus, for s large enough, we have $\psi^{s+M!}(v_q) = \psi^s(v_q)$ for all $q \in \Downarrow p$. Let a be maximal (w.r.t. the partial order of L) in the view set of $\Downarrow p$ (w.r.t. v, ψ^s). Without loss of generality (i.e. up to increasing s a bit), we can suppose that there is $q_0 \in \Downarrow p$ such that $\psi^s(v)(q_0) = a$.

Consider now the set $\{ \psi^{s+k\cdot M!}(v)(p) \mid k \geq 0 \}$ and let N be its cardinality. If, for some k, $\psi^{s+k\cdot M!}(v)(p)$ belongs to the view set of $\Downarrow p$, then, for all $q \in \Downarrow p$, $\psi^{s+k\cdot M!}(v)(q) \leq \psi^{s+k\cdot M!}(v)(p)$, and in particular $a = \psi^s(v)(q_0) = \psi^{s+k\cdot M!}(v)(q_0) \leq \psi^{s+k\cdot M!}(v)(p)$. It follows that $a = \psi^{s+k\cdot M!}(v)(p)$, by the maximality of a. Therefore, the set $\{ \psi^{s+k\cdot M!}(v)(p) \mid k \geq 0 \}$ intersects the view set of $\Downarrow p$ at most in the singleton $\{ a \}$ and, consequently, we have $M + N - 1 \leq K$, where K is the cardinality of the view set of the whole P. We clearly have that ψ^s becomes periodic in at most $N \cdot (M!)$ steps (with period bounded by this number) and the claim follows from the inequality $N \cdot (M!) \leq K!$ below. □

Lemma 30. *For $M, N \geq 1$, we have $N \cdot (M!) \leq (M + N - 1)!$.*

Proof. The case $N = 1$ is obvious, so we suppose that $N > 1$. Since $M \geq 1$, $N \leq M + N - 1$ and therefore,

$$\begin{aligned} N \cdot M! &\leq (M + N - 1)M! \\ &\leq M!(M + 1)(M + 2) \ldots (M + N - 1) = (M + N - 1)! \,, \end{aligned}$$

where for the last equality we have used that $M + N - 1 > M$. □

For a subvariety $\mathbf{V}$ of the variety of Heyting algebras, we use the notation $\mathcal{F}_{\mathbf{V}}(x_1, \ldots, x_n)$ for the free $\mathbf{V}$-algebra on the generators $x_1, \ldots, x_n$. The following result is an immediate consequence of Proposition 28:

Theorem 31. *Let $\mathbf{V}$ be a finitely approximable variety of Heyting algebras and let*

$$\mu : \mathcal{F}_{\mathbf{V}}(x_1, \ldots, x_n) \longrightarrow \mathcal{F}_{\mathbf{V}}(x_1, \ldots, x_n)$$

be an ultimately periodic endomorphism, then its period is bounded by $2^n!$.

The interesting point is that the above bound is uniform with respect to all varieties $\mathbf{V}$. However, it is not in general tight, as we shall remark in the final section by considering as $\mathbf{V}$ the variety of Boolean algebras.

Remark 32. Let us point out that the bound given in Proposition 28 strictly depends on $h_L(P)$ being a set of monotone functions. Observe that, when the bound has been constructed in the proof of Lemma 29, the function $\psi_P : h_L(P) \longrightarrow h_L(P)$ has been decomposed as $\psi_P(\underline{y}, x) = (g(\underline{y}), f(\underline{y}, x))$, where $\underline{y}$ is a vector of elements of L indexed by $\Downarrow p$ and $x \in L$; moreover, ψ is applied to pairs $(\underline{y}, x)$ such that $y \leq x$ for each $y \in \underline{y}$. If we give away the latter constraint on the

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

order, it is easy to see that the bound does not hold anymore. This happens, even when ψ is recursively defined on the height of P (so that all of its restrictions ψ_p are of the form $\langle g \circ \pi_1, f \rangle$ for some $g : \twoheaddownarrow p \longrightarrow \twoheaddownarrow p$ and for some $f : L^{\twoheaddownarrow p} \times L \to L$). Consider the following example. Let P be the chain $\{ 1, \ldots, n \}$ and let $L = \{ 0, 1 \}$, so we can identify *arbitrary* functions from P to L with words on the alphabet $\{ 0, 1 \}$ of length n. For $x \in \{ 0, 1 \}$, let $\psi_1(x) := 1 - x$. Suppose that, for $i < n$, we have defined $\psi_i : \{ 0, 1 \}^i \to \{ 0, 1 \}^i$ so that ψ_i is a bijection of period/order 2^i. We can list then $\{ 0, 1 \}^i = \{ w_0, \ldots, w_{2^i-1} \}$ with $w_j = \psi_i^j(0, \ldots, 0)$, $j = 0, \ldots, 2^i - 1$. Define then

$$\psi_{i+1}(w_j, x) := \begin{cases} (\psi_i(w_j), x), & j < 2^i - 1, \\ (\psi_i(w_j), 1 - x), & j = 2^i - 1. \end{cases}$$

This recursive construction yields ψ_n of period 2^n and, in particular, the factorial bound 2! for the period does not apply.

A subvariety $\mathbf{V}$ of Heyting algebras is said to be *locally finite* if the finitely generated free $\mathbf{V}$-algebras are all finite. Such varieties are obviously finitely approximable and the endomorphisms between finitely generated free $\mathbf{V}$-algebras are ultimately periodic, by the finiteness of these algebras. Hence, we obtain

Corollary 33. *Let* $\mathbf{V}$ *be a locally finite variety of Heyting algebras. Every endomorphism* $\mu : \mathcal{F}_{\mathbf{V}}(x_1, \ldots, x_n) \longrightarrow \mathcal{F}_{\mathbf{V}}(x_1, \ldots, x_n)$ *is ultimately periodic and its period is bounded by* $2^n!$.

Theorem 31 is, in principle, much stronger than Corollary 33, since many are the finitely approximable varieties of Heyting algebras that are not locally finite. As an example, one can take the bounded branching varieties $\mathbf{T_n}$ (for $n > 1$) of Theorem 5.53 of Chagrov and Zakharyaschev (1997). Notice that since all points of the modified Rieger–Nishimura ladder of Figure 2 have at most two successors (i.e. they have branching at most 2), the counterexample of Section 8 applies to these varieties $\mathbf{T_n}$, so they have non-ultimately periodic free algebras endomorphisms too. It is object of future research to characterize nontrivial periodic free algebra endomorphisms in finitely approximable varieties – where for nontrivial we mean that they move more than one generator.

On the other hand, if Corollary 33 has to be considered by its own, a proof of it might be devised by relying on some more common duality – we thank the anonymous referee for pointing this to us.

10. Conclusions and Open Problems

Ruitenburg's Theorem exhibits a particular finitistic behavior of one-variable substitutions in IPC. Willing to provide a semantical proof of this theorem, we have studied more general substitutions, which, algebraically, can be identified with endomorphisms of finitely generated free Heyting algebras. The proof of Ruitenburg's Theorem as well as some additional remarks on periods of iterated substitutions have been achieved using the semantical apparatus given by the sheaf theoretic duality for finitely presented Heyting algebras (Ghilardi and Zawadowski 2002).

Using these semantical tools, sheaf duality, and bounded bisimulations, we found upper bounds for the index and the period of sequences of iterated substitutions. The bounds so found are not optimal. For example, the proof of Theorem 21 yields a bound for the index which is nonelementary as a function of the implication degree of an IPC formula. On the other hand, the bound that can be extracted from the syntactic computations in Ruitenburg (1984) is linear w.r.t. the implicational degree and the number of propositional variables of a formula. The syntactic computations in Ghilardi et al. (2016, 2019) for fixpoints convergence also yield tighter bounds.

While the semantical approach has been successful for providing a proof of Ruitenburg's Theorem, it remains open whether similar approaches can yield finer bounds.

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

Other open problems arise from inspecting the results presented in this paper. Firstly, although we were able to show that periodicity fails for two-variable substitutions, it is still an open problem to characterize or to decide periodicity for arbitrary substitutions in IPC (the only sufficient condition known is the one supplied by Ruitenburg's Theorem, namely the fact that all-but-one variables are fixed).

Secondly, concerning the upper bounds we found, notice that Corollary 33 provides bounds for *periods* of free Heyting algebra endomorphisms in locally finite subvarieties; being able to bound their *indexes* might also be interesting. In particular, it is not clear whether indexes are sensitive to the number of generators of a free algebra or, similarly to what happen for fixpoint approximants in some lattice varieties, see Frittella and Santocanale (2014), they are uniform in a fixed variety. Corollary 19 can be used to argue that this is the case in varieties of Heyting algebras of bounded height – see e.g. the varieties $\mathbf{bd_n}$ in Chagrov and Zakharyaschev (1997, Prop. 2.38) – yet there are locally finite varieties of Heyting algebras – notably, the variety of Gödel–Dummett algebras – whose Kripke models might be of unbounded height.

Coming back to the period, let us also notice that the upper bound provided by Corollary 33 is not in general tight. To see why, consider free Boolean algebras: a morphism $f : \mathcal{F}_B(x_1, \ldots, x_n) \longrightarrow \mathcal{F}_B(x_1, \ldots, x_n)$ corresponds, via duality, to a function $f : \mathbf{2}^n \to \mathbf{2}^n$. Now, estimating an upper bound for the periods of functions from the set $[k] := \{1, \ldots, k\}$ (where in our case $k = 2^n$) to itself can be reduced to estimating an upper bound for the period (or order) of permutations of $[k]$. Indeed, if i and p are such that $f^{i+p} = f^i$, then the restriction of f to $f^i([k])$ is a permutation of $f^i([k])$ which can be extended to a full permutation of the set $[k]$ of equal period p. Now, an upper bound for all these periods is $\mathrm{lcm}(1, \ldots, k)$ for which we have $2^{k-1} \leq \mathrm{lcm}(1, \ldots, k) \leq 3^k$ (Farhi 2009) and, asymptotically, $\mathrm{lcm}(1, \ldots, k) \sim e^k$ (by the prime number theorem). On the other hand, using Stirling's approximation, $k! \sim \sqrt{2\pi k}(\frac{k}{e})^k$. It is an open problem whether the bound $2^n!$ can be made tighter by considering locally finite varieties of Heyting algebras other than Boolean algebras; it is not clear either how the bound can vary below $2^n!$ depending on the locally finite subvariety $\mathbf{V}$.

Finally, most of the techniques used here for Heyting algebras are also the tools for studying modal logics in Ghilardi and Zawadowski (2002). While we can expect that periodicity phenomena of substitutions do not arise for the basic modal logic $\mathbf{K}$, they surely do for locally tabular modal logics. Considering also the numerous results on definability of fixpoints, see e.g. Sambin (1976) and Alberucci and Facchini (2009), these phenomena are likely to appear in other subsystems of modal logics. As far as we know, investigation of periodicity phenomena in modal logics is a research direction which has not yet been explored and where the bounded bisimulation methods might prove their strength once more.

Acknowledgements. The authors are thankful to the anonymous referees for the careful reading and their insightful comments, by which an improved version of this manuscript was possible.

Notes

1 However, let us notice that, according to our convention, a $\langle P(\vec{x}), \supseteq \rangle$-evaluation is such that, for $p, q \in P$ if $p \leq q$ then $u(p) \supseteq u(q)$; in standard logical literature, see e.g. Chagrov and Zakharyaschev (1997), the opposite order on P is used, namely an evaluation is such that $u(q) \subseteq u(p)$, for $q \leq p$.

2 The sheaf structure becomes essential for instance when one has to compute images – images are the categorical counterparts of second-order quantifiers, see Ghilardi and Zawadowski (2002).

3 This is called "index" tout court in Ghilardi and Zawadowski (2002); here we used the word "index" for a different notion, since Section 1.

4 From now on, "periodic" will mean "2-periodic," i.e. "periodic with period 2."

5 It is easily seen that we indeed have $N_0 = N(l-1)$.

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press

References

Afshari, B. and Leigh, G. E. (2013). On closure ordinals for the modal μ-calculus. In: *Computer Science Logic 2013*, LIPIcs. Leibniz Int. Proc. Inform., vol. 23, Wadern, Schloss Dagstuhl. Leibniz-Zent. Inform., 30–44.

Alberucci, L. and Facchini, A. (2009). The modal μ-calculus hierarchy over restricted classes of transition systems. *The Journal of Symbolic Logic* **74** (4) 1367–1400.

Bellissima, F. (1986). Finitely generated free Heyting algebras. *The Journal of Symbolic Logic* **51** (1) 152–165.

Birkhoff, G. (1937). Rings of sets. *Duke Mathematical Journal* **3** (3) 443–454.

Chagrov, A. and Zakharyaschev, M. (1997). *Modal Logic*, Oxford Logic Guides, vol. 35, New York, The Clarendon Press, Oxford University Press, Oxford Science Publications.

Czarnecki, M. (2010). How fast can the fixpoints in modal μ-calculus be reached? In: Santocanale, L. (ed.) *7th Workshop on Fixed Points in Computer Science, FICS 2010*, Brno, Czech Republic, 89. Retrieved from `Hal`: https://hal.archives-ouvertes.fr/hal-00512377.

Davey, B. A. and Priestley, H. A. (2002). *Introduction to Lattices and Order*, 2nd edn., Cambridge University Press, New York.

Esakia, L. (1974). Topological Kripke models. *Soviet Mathematics - Doklady* **15** 147–151.

Farhi, B. (2009). An identity involving the least common multiple of binomial coefficients and its application. *American Mathematical Monthly* **116** (9) 836–839.

Fine, K. (1985). Logics containing K4. II. *The Journal of Symbolic Logic* **50** (3) 619–651.

Frittella, S. and Santocanale, L. (2014). Fixed-point theory in the varieties $\mathcal{D}_n$. In: Höfner, P., Jipsen, P., Kahl, W. and Müller, M. E. (eds.) *RAMICS*, Lecture Notes in Computer Science, vol. 8428, Springer, 446–462.

Ghilardi, S. (1997). Unification through projectivity. *Journal of Logic and Computation* **7** (6) 733–752.

Ghilardi, S. (1999). Unification in intuitionistic logic. *The Journal of Symbolic Logic* **64** (2) 859–880.

Ghilardi, S. (2000). Best solving modal equations. *Annals of Pure and Applied Logic* **102** (3) 183–198.

Ghilardi, S. (2004). Unification, finite duality and projectivity in varieties of Heyting algebras. *Annals of Pure and Applied Logic* **127** (1–3) 99–115. Provinces of logic determined.

Ghilardi, S., Gouveia, M. J. and Santocanale, L. (2016). Fixed-point elimination in the intuitionistic propositional calculus. In: *Foundations of Software Science and Computation Structures, FOSSACS 2016, Proceedings*, 126–141.

Ghilardi, S., Gouveia, M. J. and Santocanale, L. (2019). Fixed-point elimination in the Intuitionistic Propositional Calculus. *ACM Transactions on Computational Logic* **21** (1) 1–37.

Ghilardi, S. and Santocanale, L. (2018). Ruitenburg's theorem via duality and bounded bisimulations. In: *Advances in Modal Logic, AiML 2018, Proceedings*, 277–290.

Ghilardi, S. and Zawadowski, M. (2002). *Sheaves, Games, and Model Completions: A Categorical Approach to Nonclassical Propositional Logics*, 1st edn., Springer Publishing Company, Incorporated.

Ghilardi, S. and Zawadowski, M. W. (1997). Model completions, r-Heyting categories. *Annals of Pure and Applied Logic* **88** (1) 27–46.

Goguen, J. A. (1989). What is unification? A categorical view of substitution, equation and solution. In: *Resolution of Equations in Algebraic Structures*, vol. 1, Boston, MA, Academic Press, 217–261.

Gouveia, M. J. and Santocanale, L. (2019). $\aleph_1$ and the modal μ-calculus. *Logical Methods in Computer Science* **15** (4) 1:1–1:34.

Mardaev, S. (2007). Definable fixed points in modal and temporal logics: a survey. *Journal of Applied Non-Classical Logics* **17** (3) 317–346.

Mardaev, S. I. (1993). Least fixed points in Grzegorczyk's Logic and in the intuitionistic propositional logic. *Algebra and Logic* **32** (5) 279–288.

Milanese, G. C. and Venema, Y. (2019). Closure ordinals of the two-way modal μ-calculus. In: *Logic, Language, Information, and Computation*, Lecture Notes in Comput. Sci., vol. 11541, Berlin, Springer, 498–515.

Ruitenburg, W. (1984). On the period of sequences $(a^n(p))$ in intuitionistic propositional calculus. *The Journal of Symbolic Logic* **49** (3) 892–899.

Sambin, G. (1976). An effective fixed-point theorem in intuitionistic diagonalizable algebras. *Studia Logica* **35** (4) 345–361. The algebraization of the theories which express Theor, IX.

Shavrukov, V. Y. (1993). Subalgebras of diagonalizable algebras of theories containing arithmetic. *Dissertationes Mathematicae (Rozprawy Matematyczne)*, **323** 82.

Visser, A. (1996). Uniform interpolation and layered bisimulation. In: *Gödel '96, Brno, 1996*, Lecture Notes Logic, vol. 6, Berlin, Springer, 139–164.

Cite this article: Ghilardi S and Santocanale L (2020). Free Heyting algebra endomorphisms: Ruitenburg's Theorem and beyond. *Mathematical Structures in Computer science* **30**, 572–596. https://doi.org/10.1017/S0960129519000203

https://doi.org/10.1017/S0960129519000203 Published online by Cambridge University Press