Ruitenburg's Theorem via Duality and Bounded Bisimulations

Silvio Ghilardi

Università degli Studi di Milano, Italy

Luigi Santocanale [1]

LIS, CNRS UMR 7020, Aix-Marseille Université

Abstract

For a given intuitionistic propositional formula A and a propositional variable x occurring in it, define the infinite sequence of formulae $\{ A^i \}_{i \geq 1}$ by letting A^1 be A and A^{i+1} be $A(A^i/x)$. Ruitenburg's Theorem [8] says that the sequence $\{ A^i \}_{i \geq 1}$ (modulo logical equivalence) is ultimately periodic with period 2, i.e. there is $N \geq 0$ such that $A^{N+2} \leftrightarrow A^N$ is provable in intuitionistic propositional calculus. We give a semantic proof of this theorem, using duality techniques and bounded bisimulations ranks.

Keywords: Ruitenburg's Theorem, Sheaf Duality, Bounded Bisimulations.

1 Introduction

Let us call an infinite sequence

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

ultimately periodic iff there are N and k such that for all $s_1, s_2 \geq N$, we have that $s_1 \equiv s_2 \mod k$ implies $a_{s_1} = a_{s_2}$. If (N, k) is the smallest (in the lexicographic sense) pair for which this happens, we say that N is an *index* and k a *period* for 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 endo-function 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 stating the following: take a formula $A(x, \underline{y})$ of intuitionistic propositional calculus (IPC) (by the

[1] Partially supported by the "LIA LYSM AMU CNRS ECM INdAM"

notation $A(x, \underline{y})$ we mean that the only propositional letters occurring in A are among $x, \underline{y}$ - with $\underline{y}$ being, say, the tuple $y_1, \ldots, y_n$) and consider the sequence $\{ A^i(x, \underline{y}) \}_{i \geq 1}$ so defined:

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

where the slash means substitution; 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

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

An interesting consequence of this result is that *least (and greatest) fixpoints of monotonic formulae are definable in* (IPC) [7,6,4]: 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 fixpoints approximation convergence.

Ruitenburg's Theorem was shown in [8] 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 non classical logics [2] which is used in order to characterize satisfiability of bounded depth formulae and hence definable classes of models: examples of the use of bounded bisimulations include for instance [9], [5], [10], [3].

Duality has a long tradition in algebraic logic (see e.g. [1] for the Heyting algebras case): many phenomena look more transparent whenever they are analyzed in the dual categories, especially whenever dualities can convert coproducts and colimits constructions into more familiar 'honest' products and limits constructions. The duality we use here is taken from [5] and 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 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 combinatoric ingredients (Ehrenfeucht-Fraissé games, etc.) replace the topological ingredients which are common in the algebraic logic literature (working with arbitrary algebras instead).

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. After introducing the required duality ingredients for finitely presented Heyting algebras (this is done in Section 3 - the material of this Section is taken from [5]), we show how to extend the basic argument of Section 2 to finite Kripke models in Section 4.

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. This bound is made uniform in Section 6 (using the ranks machinery introduced in Section 5), thus finally reaching our goal.

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 need to prove that

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

holds (here A^3 is defined like 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.

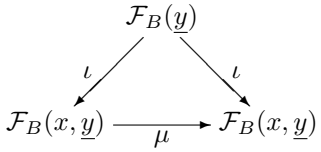
Similarly, morphisms $\mu : \mathcal{F}_B(x_1, \ldots, x_n) \longrightarrow \mathcal{F}_B(\underline{z})$ bijectively correspond to n-tuples of equivalence classes of formulae $A_1(\underline{z}), \ldots, A_n(\underline{z})$ in $\mathcal{F}_B(\underline{z})$: the map μ corresponding to the tuple $A_1(\underline{z}), \ldots, A_n(\underline{z})$ 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 composite map $\mu \circ \nu : \mathcal{F}_B(y_1, \ldots, y_m) \longrightarrow \mathcal{F}_B(\underline{z})$ is induced by the m-tuple $C_1(A_1/x_1, \ldots, A_n/x_n), \ldots, C_m(A_1/x_1, \ldots, A_n/x_n)$.

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

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

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

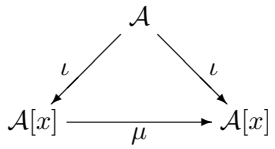


commutes.

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 $\mathcal{A}[x]$ 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 $\mathcal{A}$).

A slight generalization of statement (4) now reads as follows:

- let $\mathcal{A}$ be a finitely presented Boolean algebra [2] 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

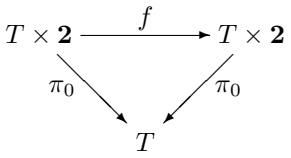
$$\mu^3 = \mu \quad . \tag{5}$$

2.2 Duality

The gain we achieved with statement (5) is that the latter is a purely categorical statement, so that we can re-interpret 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-elements 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 $\pi_0 : T \times \mathbf{2} \longrightarrow T$



Then we have

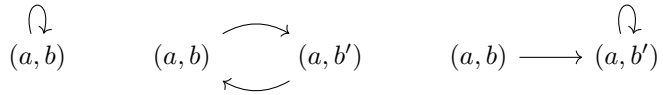
$$f^3 = f \quad . \tag{6}$$

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

[2] Recall that an algebra is finitely presented iff it is isomorphic to the quotient of a finitely generated free algebra by a finitely generated congruence. In the case of Boolean algebra 'finitely presented' is the same as 'finite', but it is not anymore like that in the case of Heyting algebras.

$f(a,b') = (a,b')$, then $f^3(a,b) = f(a,b) = (a,b')$, otherwise $f(a,b') = (a,b)$ (there are only two available values for b!) and even in this case $f^3(a,b) = f(a,b)$.

Let us illustrate these cases by thinking of the action of f on $A \times \mathbf{2}$ as one-letter deterministic automaton:



This means that on each irreducible component of the action the pairs index/period are among $(0,1)$, $(0,2)$, $(1,1)$. Out of these pairs 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 [5] concerning duality for finitely-presented Heyting algebras. Proofs of the facts stated in this section can all be found in [5, Chapter 4].

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.

Evaluations *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: we show in detail the 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 $\underline{x}$.[3] Given such a Kripke model u and an IPC formula $A(\underline{x})$, the *forcing* relation $u \models A$ is inductively defined as follows:

$$
\begin{array}{ll}
u \models x_i & \text{iff } x_i \in u(\rho(P)) \\
u \not\models \bot & \\
u \models A_1 \wedge A_2 & \text{iff } (u \models A_1 \text{ and } u \models A_2) \\
u \models A_1 \vee A_2 & \text{iff } (u \models A_1 \text{ or } u \models A_2) \\
u \models A_1 \to A_2 & \text{iff } \forall q\ (u_q \models A_1 \Rightarrow u_q \models A_2)\ .
\end{array}
$$

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 $u \sim_\infty v$).

[3] According to our conventions, we have that (for $p, q \in P$) if $p \leq q$ then $u(p) \supseteq u(q)$, that is we use $\leq$ where standard literature uses $\geq$.

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 $u(\rho(P)) = v(\rho(Q))$ (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 states a basic fact (keeping the above definition for $\sim_0$ as base case for recursion, the Proposition also supplies an alternative recursive definition for $\sim_n$):

Proposition 3.1 *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.*

It can be shown that in case $L = \mathcal{P}(x_1, \ldots, x_n)$ (i.e. when L-evaluations are just ordinary finite Kripke models over the language built up from the propositional variables $x_1, \ldots, x_n$), two evaluations are $\sim_\infty$-equivalent (resp. $\sim_n$-equivalent) iff they force the same formulas (resp. the same formulas up to implicational degree n). This can be explained in a formal way as follows. For an IPC formula $A(\underline{x})$, define the *implicational degree* $d(A)$ 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) $d(A_1 \to A_2) = max[d(A_1), d(A_2)] + 1$.

Then one can prove [10] that: (1) $u \sim_\infty v$ holds precisely iff $(u \models A \Leftrightarrow v \models A)$ holds for all formulae $A(\underline{x})$; (2) for all n, $u \sim_n v$ holds precisely iff $(u \models A \Leftrightarrow v \models A)$ holds for all formulae $A(\underline{x})$ with $d(A) \leq n$.[4]

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,

[4] For the statement (1) to be true, it is essential our evaluations to be defined over *finite* posets.

however, we also need a geometric environment, which we introduce using presheaves.

Recall that posets can be viewed as topological spaces whose open subsets are the downward closed subsets. If P, Q are posets, then a map $f : Q \longrightarrow P$ is continuous iff it is order-preserving and open in the topological sense iff it satisfies the following condition forall $q \in Q, p \in P$

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

We shall consider continuous open maps between finite posets and say that rest that $f : Q \longrightarrow P$ is *open* iff it is order-preserving and moreover open in the topological sense. [5]

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, that is, 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 to each finite rooted poset P 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 won't need this fact, [6] but we nevertheless call h_L the *sheaf of L-evaluations* (presheaves of the kind h_L, for some L, are called *evaluation sheaves*).

Notice the following fact: 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 $\mathbf{P_0}$); thus, we shall feel free to use the (non-ambiguous) notation $\psi(v)_p$ to denote $\psi(v_p) = (\psi(v))_p$.

The notion of *bounded bisimulation index* (*b-index*, for short) [7] takes to-

---

[5] Open surjective maps are called p-morphisms in the standard non classical logics terminology.

[6] The sheaf structure becomes essential for instance when one has to compute images - images are the categorical counterparts of second order quantifiers, see [5].

[7] This is called 'index' tout court in [5]; here we used the word 'index' for a different notion, since Section 1.

gether structural and combinatorial aspects. We say that a natural transformation $\psi : h_L \longrightarrow h_{L'}$ *has b-index* n iff 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 do compose):

Proposition 3.2 *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 $\psi(v) \sim_k \psi(v')$.*

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 just state a duality for the intermediate category of Heyting algebras freely generated by a finite bounded distributive lattice (this is quite simple to state and is sufficient for proving Ruitenburg's Theorem).

Theorem 3.3 *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 leave for an extended version of this paper a proof of the above Theorem (such a proof is contained in [5] and does not play a role in the sequel), however we give some hints on how to reconstruct it. Say that a sub-presheaf S of h_L is *definable* if, for some $n \geq 0$, $v \in S(P)$ and $v \sim_n u$ imply $v \in S(Q)$ (P, Q are the domains of v, u respectively). Such a sub-presheaf corresponds to the set of finite models of a propositional formula. It turns out that a natural transformation f has a b-index iff the inverse image along f of a definable sub-presheaf is definable: *precisely such maps are the duals of substitutions*.

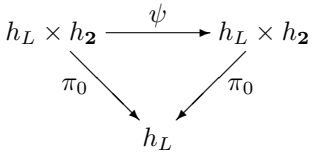
It is important to notice that in the subcategory mentioned in the above Theorem 3.3, products are computed as in the category of presheaves. This means that they are computed pointwise, like in the category of sets: in other words, we have that $(h_L \times h_{L'})(P) = h_L(P) \times h_{L'}(P)$ and $(h_L \times h_{L'})(f) = h_L(f) \times h_{L'}(f)$, for all P and 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 [1] for example, for which 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 3.4 *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 $1 \leq 0$.*

4 Indexes and Periods over Finite Models

Taking into consideration the algebraic reformulation from Section 2 and the information from the previous section, 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 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 $\psi = \langle \pi_0, \chi \rangle$, where 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; we assume that $n \geq 1$ is a b-index for both of them. Incidentally, since projections have b-index 0, we can take n to be a b-index of χ. *We let such $\psi = \langle \pi_0, \chi \rangle$ and n be fixed for the rest of the paper.*

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

$$u_0 := u \quad \text{and} \quad u_{k+1} := \chi(v, u_k)\,. \tag{7}$$

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 $(v, u) \in h_L(P)$, 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 on P, thus proving Ruitenburg's Theorem).

Call $(v, u) \in h_L(P) \times h_{\mathbf{2}}(P)$ *2-periodic* (or just *periodic*[8]) iff we have $\psi^2(v, u) = (v, u)$; 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 4.1 *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 $u_1(p) = \chi(u, v)(p) = 0$.*

[8] From now on, 'periodic' will mean '2-periodic', i.e. 'periodic with period 2'.

Proof. We work by induction on the height of p (i.e. on the maximum $\leq$-chain starting with p in P). If the height of p is 1, then the argument is the same as in the classical logic case (see Section 2).

If the height is greater than one, then we need a simple combinatorial check about the possible cases that might arise. Recalling the above definition (7) of the **2**-evaluations u_n, the induction hypothesis implies that there is M big enough so that so for all $k \geq M$ and $q < p$, $(u_{k+2})_q = (u_k)_q$.

Let $\Downarrow p = \{\, q \in P \mid q < p \,\}$. We shall represent $(u_k)_p$ as a pair $\binom{a_k}{x_k}$, where $a_k = u_k(p)$ and x_k is the restriction of $(u_k)_p$ to $\Downarrow p$.

Let us start by considering a first repeat (i, j) of the sequence $\{\, a_{M+k} \,\}_{k\geq 0}$ - that is i is the smallest i such that there is $j > 0$ such that $a_{M+i+j} = a_{M+i}$ and j is the smallest such j. Since the a_{M+n} can only take value 0 or 1, we must have $i+j \leq 2$. We show that the sequence $\{\, (u_{M+k})_p \,\}_{k\geq 0}$ 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 $x = x_M$ and $y = x_{M+1}$ (recall that we do now know whether $x = y$).

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

$$(u_M)_p = \binom{a}{x},\ (u_{M+1})_p = \binom{b}{y},\ (u_{M+2})_p = \binom{a}{x}\,.$$

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

$$(u_M)_p = \binom{a}{x},\ (u_{M+1})_p = \binom{a}{y},\ (u_{M+2})_p = \binom{c}{x},\ (u_{M+3})_p = \binom{d}{y}\,.$$

If $x = y$, then we have a repeat at $(0, 1)$. Also, if $a = 1$, then the mappings x and y are uniformly 1, [9] so 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 $j = 1$):

$$(u_M)_p = \binom{a}{x},\ (u_{M+1})_p = \binom{b}{y},\ (u_{M+2})_p = \binom{b}{x},\ (u_{M+3})_p = \binom{d}{y}\,.$$

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. □

[9] Recall that our evaluations are order-preserving maps and we have $1 \leq 0$ in **2**.

Corollary 4.2 *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. □

5 Ranks

Ranks (already introduced in [2]) are a powerful tool suggested by 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

$$\langle [(v_p, u_p)]_{n-1}, [\psi(v_p, u_p)]_{n-1} \rangle. \tag{8}$$

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 (8) coming from a periodic point just get swapped after applying ψ. A non-periodic point $p \in P$ has *minimal rank* iff we have $rk(p) = rk(q)$ for all non-periodic $q \leq p$.

Lemma 5.1 *Let $p \in P$ be a non-periodic point of minimal rank in $(v,u) \in h_L(P) \times h_{\mathbf{2}}(P)$; 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

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

(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 theorem 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 3.2 $\psi^{m+1}(v,u)_q \sim_0 \psi^{m+1}(v,u)_{q'}$, for all $q, q' \in \Pi^c$; that is, ψ^{m+1} is constant on Π^c. □

6 Ruitenburg's Theorem

We can finally prove:

Theorem 6.1 (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 $p \in dom(v,u)$ such that $l \geq |v(p)|$, we have that $\psi^{N(l)}(v_p, u_p)$ is periodic.* Once this is proved, the statement of the Theorem shall be proved with $N = N(|L|)$.[10]

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 $l_0 < l$:[11] 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 means 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).

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

[10] It will turn out that $N(l)$ is $2R(l-1)+1$.

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

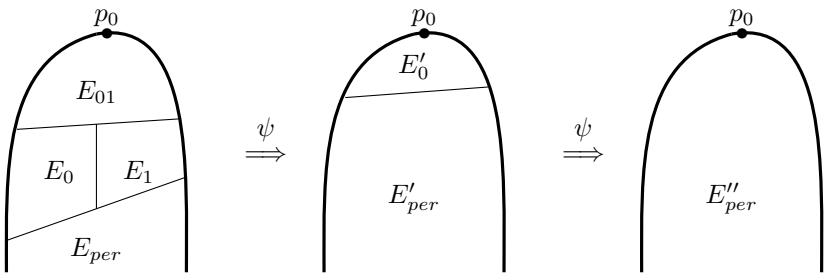
the choice of N_0 above). Let us divide the points of $\downarrow p_0$ into four subsets:

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

Let us define a *frontier point* to be a non-periodic point $f \leq p$ such that all $q < f$ are periodic. Notice that, since all the elements strictly below a frontier point f are periodic, such an f belongs to E_i, where $i = u_0(f)$. Therefore, by Lemma 4.1, 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 5.1 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 4.1.

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. □



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.

The above proof of Theorem 6.1 gives a bound for N which is not optimal, when compared with the bound obtained via syntactic means in [8] (the syntactic computations in [4] for fixpoints convergence are also better). Thus refining indexes of ultimate periodicity of our sequences within semantic arguments remains as an open question.

References

[1] Esakia, L., *Topological Kripke models*, Soviet Math. Dokl. **15** (1974), pp. 147–151.
[2] Fine, K., *Logics containing* K4. *II*, J. Symbolic Logic **50** (1985), pp. 619–651.
[3] Ghilardi, S., *Best solving modal equations*, Ann. Pure Appl. Logic **102** (2000), pp. 183–198.
[4] Ghilardi, S., M. J. Gouveia and L. Santocanale, *Fixed-point elimination in the intuitionistic propositional calculus*, in: *Foundations of Software Science and Computation Structures, FOSSACS 2016, Proceedings*, 2016, pp. 126–141.
[5] Ghilardi, S. and M. Zawadowski, "Sheaves, Games, and Model Completions: A Categorical Approach to Nonclassical Propositional Logics," Springer Publishing Company, Incorporated, 2011, 1st edition.
[6] Mardaev, S., *Definable fixed points in modal and temporal logics: A survey*, Journal of Applied Non-Classical Logics **17** (2007), pp. 317–346.
[7] Mardaev, S. I., *Least fixed points in Grzegorczyk's Logic and in the intuitionistic propositional logic*, Algebra and Logic **32** (1993), pp. 279–288.
[8] Ruitenburg, W., *On the period of sequences* $(a^n(p))$ *in intuitionistic propositional calculus*, The Journal of Symbolic Logic **49** (1984), pp. 892–899.
[9] Shavrukov, V. Y., *Subalgebras of diagonalizable algebras of theories containing arithmetic*, Dissertationes Math. (Rozprawy Mat.) **323** (1993), p. 82.
[10] Visser, A., *Uniform interpolation and layered bisimulation*, in: *Gödel '96 (Brno, 1996)*, Lecture Notes Logic **6**, Springer, Berlin, 1996 pp. 139–164.