Automated Compositional Reasoning of Intuitionistically Closed Regular Properties*

Yih-Kuen Tsay[1] and Bow-Yaw Wang[2]

[1] Department of Information Management, National Taiwan University, Taiwan
[2] Institute of Information Science, Academia Sinica, Taiwan

Abstract. Analysis of infinitary safety properties with automated compositional reasoning through learning is discussed. We consider the class of intuitionistically closed regular languages and show that it forms a Heyting algebra and is finitely approximatable. Consequently, compositional proof rules can be verified automatically and learning algorithms for finitary regular languages suffice for generating the needed contextual assumptions. We also provide a semantic justification of an axiom to deduce circular compositional proof rules for such infinitary languages.

1 Introduction

Compositional reasoning is probably the best way to harness complexity in formal verification [7]. It reduces complexity by decomposing systems into components according to compositional proof rules. In the assume-guarantee paradigm, each component is verified separately with auxiliary contextual assumptions. With an adequate degree of automation, compositional reasoning is also seen by many as an effective technique to alleviate the state explosion problem in model checking. One approach to full automation based on learning has been proposed in [6, 5]. In the approach, system behaviors and properties are restricted to regular languages and the needed contextual assumptions are generated by a learning algorithm. It is possible in theory to extend automated compositional reasoning based on learning to ω-regular languages [8]. However, it is not clear how this extension can be made practically usable. The learning algorithm in [8] generates ω-automata by posing membership and equivalence queries, the latter of which are computationally expensive for ω-regular languages.

A natural question to ask is whether automated compositional reasoning can be generalized to some subclass of ω-regular languages while maintaining practical feasibility. In particular, one may consider the class of closed ω-regular languages, which corresponds to the class of safety properties and is of fundamental importance in formal specification. Unfortunately, this subclass of ω-regular languages does not form a Boolean algebra [14]. Developing compositional proof

* The work is partly supported by NSC grant 96-3114-P-001-002-Y. The second author is also supported by NSC grant 95-2221-E-001-024-MY3 and the SISARL thematic project of Academia Sinica.

rules for the subclass is more involved. Moreover, weakest contextual assumptions may not be generated by learning algorithms because they may not belong to the subclass. Automated compositional reasoning therefore may not work even if compositional proof rules are available [6].

In this paper, we extend automated compositional reasoning to the class of intuitionistically closed regular languages. An intuitionistically closed regular language contains all (finite) prefixes of ω-strings in its corresponding closed ω-regular language. Finite approximations in an intuitionistically closed regular language allow to characterize its ω-strings. Learning algorithms for regular languages suffice to generate contextual assumptions for the class efficiently. Furthermore, we are able to show the class of intuitionistically closed regular languages forms a Heyting algebra. Compositional proof rules can thus be deduced automatically [1, 18]. Automated compositional reasoning is therefore generalized to the class of intuitionistically closed regular languages without any penalty.

The intuitionistic interpretation additionally admits circular compositional proof rules. Circularity in compositional reasoning has been observed in various models of reactive systems (see, for example, [3]). For intuitionistically closed regular languages, we are able to establish the same circular compositional proof rule in [1, 18]. More circular compositional proof rules can be established syntactically. The combination of automata and proof theory hence relieves users from making tedious inductive proofs for circular reasoning.

It is practically impossible to enumerate all works related to compositional reasoning. Readers are referred to [7] for a thorough introduction. The learning algorithm L^* for regular languages was introduced in [4]. It generates the minimal finite state automaton for an unknown regular language with a polynomial number of membership and equivalence queries. Applying the L^* algorithm to compositional reasoning was first proposed in [6].

Introductions to infinitary languages can be found in [15, 14]. Closed ω-regular languages were characterized by Landweber [10, 17, 14]. The learning algorithm L^ω for ω-regular languages in the intersection of Borel classes F_σ and G_δ was introduced in [12]. However, the algorithm L^ω requires asymptotically more queries than L^*. In [8], a learning algorithm for general ω-regular languages is introduced. It may make an exponential number of queries, though.

In [1], a finitary intuitionistic interpretation was proposed to derive proof rules in compositional reasoning. An effective version of the interpretation had been developed and applied in automated compositional reasoning [18]. An infinitary intuitionistic interpretation for linear temporal logic was introduced in [11]. None generalizes automated compositional reasoning to infinitary languages.

The paper is organized as follows. After the introduction, some backgrounds are given in Section 2. The following section presents the negative result for closed ω-regular languages. Infinitary regular languages under intuitionistic interpretation are introduced in Section 4. The correspondence between Landweber automata and intuitionistically closed regular languages is given in Section 5. Section 6 shows that the class of intuitionistically closed regular languages forms

a Heyting algebra. Applications to automated compositional reasoning are presented in Section 7. We conclude this paper in Section 8.

2 Preliminaries

A *partially ordered set* $(P, \leq)$ consists of a set P and a reflexive, anti-symmetric, and transitive binary relation $\leq \subseteq P \times P$ [9]. A *lattice* $(L, \leq, \sqcup, \sqcap)$ is a partially ordered set where the *least upper bound* $a \sqcup b$ and the *greatest lower bound* $a \sqcap b$ with respect to $\leq$ exist for any pair of elements a, b in L. A *Boolean algebra* $(B, \leq, \sqcup, \sqcap, -, 0, 1)$ is a lattice such that (1) $0 \leq a$ and $a \leq 1$ for all $a \in B$; (2) $a \sqcup -a = 1$, $a \sqcap -a = 0$ for all $a \in B$; and (3) $a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c)$ and $a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$ for all $a, b, c \in B$. The Boolean domain $\mathbb{B} = \{\mathsf{false}, \mathsf{true}\}$ forms the Boolean algebra $(\mathbb{B}, \Rightarrow, \vee, \wedge, \bar{\bullet}, \mathsf{false}, \mathsf{true})$.

A *Heyting algebra* $(H, \leq, \sqcup, \sqcap, \Rightarrow, 0, 1)$ is a lattice where (1) $0 \leq a$ and $a \leq 1$ for all $a \in H$; and (2) for all $a, b \in H$, the *pseudo-complement of a relative to b*, $a \Rightarrow b$, satisfies

$$\text{for all } c \in H, c \leq (a \Rightarrow b) \text{ if and only if } c \sqcap a \leq b.$$

Let Σ be an *alphabet* consisting of a finite set of *symbols*. A *string* α is a finite sequence of symbols. We say α is a string of *length* n (denoted by $|\alpha| = n$) if $\alpha = \alpha(1)\alpha(2)\cdots\alpha(n)$. The *empty string* λ is the string of length zero. The set of all strings is denoted by Σ^*. An *ω-string* $\xi = \xi(1)\xi(2)\cdots\xi(i)\cdots$ is an infinite sequence of symbols with length $|\xi| = \omega$ by convention. We denote the set of all ω-strings by Σ^ω and define $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$. A *language* is a subset of Σ^*; an *ω-language* is a subset of Σ^ω; and an *intuitionistic language* is a subset of Σ^∞.

Let $\sigma, \tau \in \Sigma^\infty$. We say σ is a *prefix* of τ (written $\sigma \sqsubseteq \tau$) if $\tau = \sigma\nu$ for some $\nu \in \Sigma^\infty$, or $\sigma = \tau$. For any $\sigma \in \Sigma^\infty$, define $\mathbf{A}(\sigma) = \{\tau \in \Sigma^\infty : \tau \sqsubseteq \sigma\}$. It is routine to generalize the definition over any intuitionistic language X by taking $\mathbf{A}(X) = \{\tau \in \Sigma^\infty : \tau \sqsubseteq \sigma \text{ for some } \sigma \in X\}$. An intuitionistic language $X \subseteq \Sigma^\infty$ is *prefix-closed* if $\mathbf{A}(X) \subseteq X$.

Given an intuitionistic language $X \subseteq \Sigma^\infty$, define its *classical closure* $\mathbf{cl}_\omega(X)$ to be $\{\xi \in \Sigma^\omega : \mathbf{A}(\xi) \cap \Sigma^* \subseteq \mathbf{A}(X)\}$. For any ω-language L, we say it is *classically closed* if $\mathbf{cl}_\omega(L) = L$. The class of classically closed ω-languages is denoted by $\mathcal{F}_\omega$. It is known that classically closed ω-languages correspond to safety properties [2]. Similarly, define the *intuitionistic closure* $\mathbf{cl}_\infty(X) = \{\sigma \in \Sigma^\infty : \mathbf{A}(\sigma) \cap \Sigma^* \subseteq \mathbf{A}(X)\}$ for any intuitionistic language $X \subseteq \Sigma^\infty$. An intuitionistic language X is *intuitionistically closed* if $\mathbf{cl}_\infty(X) = X$. We write $\mathcal{F}_\infty$ for the class of intuitionistically closed languages. Note that $X \subseteq \mathbf{cl}_\infty(X)$ for $X \in \Sigma^\infty$ and $L \subseteq \mathbf{cl}_\omega(L)$ for $L \in \Sigma^\omega$. Moreover, $\mathbf{cl}_\omega(X) \subseteq X$ if $X \in \mathcal{F}_\infty$.

An intuitionistic language may not be intuitionistically closed even if its ω-strings form a classically closed ω-language. Consider $X = (01)^* \subseteq \Sigma^\infty$ where $\Sigma = \{0, 1\}$. $X \cap \Sigma^\omega = \emptyset$ is classically closed. But the completion of its strings $(01)^\omega$ is not in X. Hence X is not intuitionistically closed.

An *automaton* $M = (\Sigma, Q, q_0, \delta, F)$ consists of an alphabet Σ, a finite set of *states* Q, an *initial state* $q_0 \in Q$, a *transition relation* $\delta \subseteq Q \times \Sigma \times Q$, and a set of

accepting states $F \subseteq Q$. For clarity, we write $q \xrightarrow{a} q'$ if $(q, a, q') \in \delta$. Moreover, we say the automaton M is *deterministic* if its transition relation is in fact a function from $Q \times \Sigma$ to Q. Given $\sigma \in \Sigma^\infty$ and an automaton M, a *run of* M *on* σ is a sequence of states $q_0 q_1 \cdots q_i \cdots$ such that $q_0 \xrightarrow{\sigma(1)} q_1 \cdots q_i \xrightarrow{\sigma(i+1)} q_{i+1} \cdots$. The set $Run_M(\sigma)$ contains runs of M on σ; it is a singleton if M is deterministic.

Let $M = (\Sigma, Q, q_0, \delta, F)$ be an automaton and $\alpha \in \Sigma^*$ with $|\alpha| = n$. A run $r = q_0 q_1 \cdots q_n \in Run_M(\alpha)$ satisfies the *finite acceptance condition* if $q_n \in F$. The automaton M *accepts* α if r satisfies the finite acceptance condition for some $r \in Run_M(\alpha)$. The set of strings accepted by M with finite acceptance condition forms a language $L_*(M)$. A language L in Σ^* is *regular* if $L = L_*(M)$ for some automaton M. The class of regular languages is denoted by $\mathcal{R}_*$.

Let $M = (\Sigma, Q, q_0, \delta, F)$ be an automaton, $\xi \in \Sigma^\omega$, and $r \in Run_M(\xi)$. Define $Inf_M(r) = \{q : q \text{ occurs infinitely often in } r\}$. We say r satisfies the *Büchi acceptance condition* if $Inf_M(r) \cap F \neq \emptyset$. Similarly, define $Rng_M(r) = \{q : q \text{ occurs in } r\}$. We say r satisfies the *Landweber acceptance condition* if $Rng_M(r) \subseteq F$. A *Büchi automaton* is an automaton $B = (\Sigma, Q, q_0, \delta, F)$ with the Büchi acceptance condition. It *accepts* the ω-language $L_\omega(B) = \{\xi \in \Sigma^\omega : Inf_B(r) \cap F \neq \emptyset \text{ for some } r \in Run_B(\xi)\}$. The class of ω-languages accepted by Büchi automata are denoted by $\mathcal{R}_\omega$. A *Landweber automaton* is a deterministic automaton $R = (\Sigma, Q, q_0, \delta, F)$ with the Landweber acceptance condition. It *accepts* the ω-language $L_\omega(R) = \{\xi \in \Sigma^\omega : Rng_R(r) \subseteq F \text{ for the } r \in Run_R(\xi)\}$.

Theorem 1. *[10, 14] Let $L \subseteq \Sigma^\omega$. $L \in \mathcal{R}_\omega \cap \mathcal{F}_\omega$ if and only if $L = L_\omega(R)$ for some Landweber automaton R.*

Let M and P be automata. The *language containment problem* is to decide whether $L_\bullet(M) \subseteq L_\bullet(P)$. In the automata-theoretic approach to formal verification, system behaviors and requirements are specified by the languages accepted by automata M and P respectively. Hence the conformance of the system M with respect to the requirement P is reduced to the language containment problem [16]. Oftentimes, a system is specified by the composition of its components; its behaviors are defined as the intersection of those of its components [6, 18]. The number of states therefore grows exponentially in compositions. An effective solution to the state explosion problem is compositional reasoning.

In compositional reasoning, compositional proof rules are used to deduce the correctness of a system by parts. A *compositional proof rule* is of the form

$$\ell \; \frac{\Gamma_0, \Gamma_1, \ldots, \Gamma_n}{\Delta} \; \mathcal{C}$$

where ℓ is its *label*, $\mathcal{C}$ is a *side condition*, $\Gamma_0, \Gamma_1, \ldots, \Gamma_n$, and Δ are instances of the language containment problem. The instances $\Gamma_0, \Gamma_1, \ldots, \Gamma_n$ are the *premises* of the compositional proof rule; Δ is the *conclusion*. A compositional proof rule is *sound* if its conclusion follows from its premises; it is *invertible* if all its premises are satisfiable provided its conclusion holds.

3 Compositional Reasoning of Classically Closed Languages

In the assume-guarantee paradigm of compositional reasoning, users are allowed to specify contextual assumptions in premises of compositional proof rules. If the compositional proof rule is sound and invertible, users are guaranteed to find proper assumptions to verify the system. Finding proper assumptions nevertheless is tedious and often requires clairvoyance. Automated compositional reasoning applies machine learning to generate assumptions for users automatically. Consider the following compositional proof rule, where system behaviors and property are formalized as regular languages J, K, and L respectively [5]:

$$R0\ \frac{J \cap A \subseteq L \qquad K \subseteq A}{J \cap K \subseteq L}$$

Since regular languages are closed under Boolean operations, learning algorithms gradually converge to the weakest assumption $L \cup \overline{J}$ through a series of membership and equivalence queries. These queries are reduced to membership and language containment problems and then resolved automatically.

Extending the automated methodology to ω-regular languages does not look promising. The only learning algorithm for general ω-regular languages may make an exponential number of queries [8]. Moreover, the language containment problem for ω-regular languages is computationally harder than for regular languages. Even if one considers the subclass with efficient learning algorithms [12], resolving equivalence queries for ω-regular languages is still less efficient.

The outlook does not improve for the most important class of classically closed ω-regular languages. Consider again the compositional proof rule *R0*. Suppose now J, K, L are classically closed ω-regular languages. The weakest assumption $\overline{J} \cup L$ is not necessarily classically closed since the class of classically closed ω-regular languages is not closed under complementation. It is too restrictive to consider only the class of classically closed ω-regular languages. One wonders whether the weakest assumption is defined too liberally. If only assumptions in the class of classically closed ω-regular languages are considered, could the weakest assumption exist? Algebraically, the weakest assumption is but the pseudo-complement of J relative to L. It is however not hard to see that the weakest assumption does not always exist.

Proposition 1. *For some $K, L \in \mathcal{R}_\omega \cap \mathcal{F}_\omega$, there is no $C \in \mathcal{R}_\omega \cap \mathcal{F}_\omega$ such that for all $J \in \mathcal{R}_\omega \cap \mathcal{F}_\omega$, $J \cap K \subseteq L$ if and only if $J \subseteq C$.*

Proposition 1 suggests that automated compositional reasoning cannot be applied to classically closed ω-regular languages naïvely. In the following, we propose a new class of infinitary languages suitable for the automated technique.

4 Intuitionistic Regular Languages

To motivate the intuitionistic interpretation, consider the ω-languages $K = (01)^\omega$ and $L = \emptyset$. We would like to find the maximal classically closed ω-language

J such that $J \cap K \subseteq L$. Observe that the ω-language $J_i = (01)^i 0^\omega$ satisfies $J_i \cap K \subseteq \emptyset$ for $i \in \mathbb{N}$. Hence $J_i \subseteq J$ for $i \in \mathbb{N}$. But one would have $(01)^\omega \in J$ and $J \cap K \neq \emptyset$ for J is classically closed.

One way to circumvent the problem is to disallow J_i's. Notice that $\mathbf{A}(J_i) \cap \mathbf{A}(K) \neq \emptyset$ though $J_i \cap K = \emptyset$ for each i. Indeed, $\cup_{i \in \mathbb{N}} \mathbf{A}(J_i)$ and the closure property imply $(01)^\omega \in J$. If prefixes of ω-languages were taken into consideration, the embarrassing dilemma would disappear.

The idea is best illustrated automata-theoretically. Recall that automata for finitary and infinitary languages are indistinguishable structurally; only their acceptance conditions differ. We therefore generalize the language accepted by an automaton to the new interpretation.

Definition 1. *Let B be a Büchi automaton. Define*

$$L_\infty(B) = \{\sigma \in \Sigma^\infty : B \textit{ accepts } \sigma \textit{ by finite or Büchi acceptance condition}\}$$
$$\mathcal{R}_\infty = \{X \subseteq \Sigma^\infty : X = L_\infty(B) \textit{ for some Büchi automaton } B\}.$$

Unlike classical ω-regular languages, intuitionistic regular languages do not form a Boolean algebra. To apply automated compositional reasoning, one could try to form a Heyting algebra over intuitionistic regular languages [18].

5 Landweber Automata and Intuitionistically Closed Regular Languages

Recall that the class of ω-languages accepted by Landweber automata coincides with the class of classically closed ω-regular languages (Theorem 1). We consider strings accepted by finite acceptance condition as well.

Definition 2. *Let R be a Landweber automaton. Define $L_\infty(R) = \{\sigma \in \Sigma^\infty : Rng_R(r) \subseteq F$ for the $r \in Run_R(\sigma)\}$.*

The following lemma states the intuitionistic language accepted by a Landweber automaton is indeed intuitionistically regular.

Lemma 1. *Let R be a Landweber automaton. $L_\infty(R) \in \mathcal{R}_\infty$.*

To show $L_\infty(R)$ is intuitionistically closed for any Landweber automaton R, consider the infinite run for any ω-string in $\mathbf{cl}_\infty(L_\infty(R))$. It only visits accepting states since all prefixes of the ω-string belong to $L_\infty(R)$. Hence only accepting states can occur in the infinite run. The ω-string belongs to $L_\infty(R)$ as well.

Lemma 2. *Let R be a Landweber automaton. $L_\infty(R)$ is intuitionistically closed.*

Recall that intuitionistic regular languages are defined by (non-deterministic) Büchi automata but intuitionistically closed regular languages are by (deterministic) Landweber automata. To show that any intuitionistically closed regular language is accepted by a Landweber automaton, one must close the gap between deterministic and non-deterministic computation. Since there is no gap in classically closed ω-regular languages (Theorem 1), one would not expect differently in our intuitionistic interpretation.

Lemma 3. *Let $X \in \mathcal{R}_\infty$. If X is intuitionistically closed, $X = L_\infty(B)$ for some deterministic Büchi automaton B.*

It is not hard to translate deterministic Büchi automata to Landweber automata. The correspondence between intuitionistically closed regular languages and intuitionistic languages accepted by Landweber automata is obtained.

Theorem 2. *For any $X \subseteq \Sigma^\infty$, $X \in \mathcal{R}_\infty \cap \mathcal{F}_\infty$ if and only if $X = L_\infty(R)$ for some Landweber automaton R.*

6 Intuitionistically Closed Regular Languages as Heyting Algebra

We first characterize pseudo-complements. Given $X, Y \in \Sigma^\infty$, the language $X \to Y$ consists of strings whose every prefixe, if in X, also belongs to Y.

Definition 3. *[11] Let $X, Y \in \Sigma^\infty$. $X \to Y = \{\sigma \in \Sigma^\infty : \mathbf{A}(\sigma) \cap X \subseteq Y\}$.*

We now show that $X \to Y$ is intuitionistically closed regular if both X and Y are. Since X and Y are intuitionistically closed regular languages, they are accepted by Landweber automata R and S respectively. We define a Landweber automaton $R \to S$ such that $L_\infty(R \to S) = L_\infty(R) \to L_\infty(S) = X \to Y$.

Definition 4. *Let $R = (\Sigma, P, p_0, \phi_R, F_R)$ and $S = (\Sigma,\ Q,\ q_0,\ \phi_S,\ F_S)$ be Landweber automata. Define the Landweber automaton $R \to S = (P \times Q \times \mathbb{B}, (p_0, q_0, b_0), \phi, F)$ as follows.*

- $b_0 = \mathsf{true}$ *if and only if* $p_0 \in F_R$ *implies* $q_0 \in F_S$
- $(p', q', b') = \phi((p, q, b), a)$ *if*
  - $p' = \phi_R(p, a)$, $q' = \phi_S(q, a)$, *and*
  - $b' = \mathsf{true}$ *if and only if* $b = \mathsf{true}$, *and* $p' \in F_R$ *implies* $q' \in F_S$.
- $F = \{(p, q, \mathsf{true}) : p \in P, q \in Q\}$.

By construction, the language $L_\infty(R \to S)$ is prefix-closed. Moreover, a string is in $L_\infty(R \to S)$ if all its finite prefixes belong to $L_\infty(R \to S)$ since $L_\infty(R \to S)$ is intuitionistically closed. We can now show $L_\infty(R \to S) = L_\infty(R) \to L_\infty(S)$.

Proposition 2. *Let R and S be Landweber automata. $L_\infty(R \to S) = L_\infty(R) \to L_\infty(S)$.*

To summarize, we have shown the language $K \to L$ is intuitionistically closed regular if both K and L are intuitionistically closed regular.

Corollary 1. *If $X, Y \in \mathcal{R}_\infty \cap \mathcal{F}_\infty$, $X \to Y \in \mathcal{R}_\infty \cap \mathcal{F}_\infty$.*

It is easy to verify $\emptyset$ and Σ^∞ are both intuitionistically closed regular. Moreover, $X \cup Y$, $X \cap Y$, and $X \to Y$ are intuitionistically closed regular if both X and Y are. Hence the class $\mathcal{R}_\infty \cap \mathcal{F}_\infty$ forms a Heyting algebra.

Theorem 3. $(\mathcal{R}_\infty \cap \mathcal{F}_\infty, \subseteq, \cup, \cap, \rightarrow, \emptyset, \Sigma^\infty)$ *is a Heyting algebra.*

A simple application of elementary proof theory allows to establish sound and invertible compositional proof rules [1, 18].

Corollary 2. *If a compositional proof rule is provable by the system LJ, it is sound and invertible for intuitionistically closed regular languages.*

Particularly, the rule given in Section 3 is sound and invertible for $\mathcal{R}_\infty \cap \mathcal{F}_\infty$. Moreover, the weakest assumption $J \rightarrow L$ is in fact an intuitionistically closed regular language by Theorem 3. A learning algorithm for intuitionistically closed regular languages can generate a Landweber automaton accepting $J \rightarrow L$. The termination of automated compositional reasoning is thus ensured.

Circularity in compositional proof rules is always intriguing because it contradicts our intuition. Consider the following rule where $\mathcal{C}$ is a side condition [3].

$$\frac{J_0 \cap K_1 \subseteq K_0 \qquad K_0 \cap J_1 \subseteq K_1}{J_0 \cap J_1 \subseteq K_0 \cap K_1}\ \mathcal{C}$$

Circular reasoning arises because the premise $J_0 \cap K_1 \subseteq K_0$ assumes K_1 to establish K_0 and the other assumes K_0 to establish K_1. Circular reasoning is not sound for Heyting algebra in general. But the class $\mathcal{R}_\infty \cap \mathcal{F}_\infty$ admits such circularity conditionally. The following definition is needed to describe the condition.

Definition 5. *Let $X \subseteq \Sigma^\infty$ and $\Xi \subseteq \Sigma$. X is said to* constrain *Ξ (write $X \triangleright \Xi$) if $\alpha a \in X$ for any $\alpha \in X \cap \Sigma^*$ and $a \notin \Xi$.*

Definition 5 intuitively says that a language X is not interfered by the symbols not in Ξ if $X \triangleright \Xi$. If two languages are not interfering with each other, one can apply the following lemma to have circular compositional proof rules.

Lemma 4. *Let $X, Y \in \mathcal{F}_\infty$ with $X, Y \neq \emptyset$, and $\Xi_X, \Xi_Y \subseteq \Sigma$. If $X \triangleright \Xi_X$, $Y \triangleright \Xi_Y$, and $\Xi_X \cap \Xi_Y = \emptyset$, then $(X \rightarrow Y) \cap (Y \rightarrow X) \subseteq X$.*

Note that Lemma 4 is only applicable to non-empty intuitionistically closed languages. It is necessary since the pseudo-complement of the empty language is Σ^∞. Fortunately, the class of non-empty intuitionistically closed regular languages still forms a Heyting algebra with the minimal element $\{\lambda\}$. The circular compositional proof rule described above can thus be established by the system LJ and Lemma 4 (see also [1, 18]).

7 Applications

An advantageous feature of intuitionistically closed regular languages is that they contain finite approximations and their completions. If one could infer more information from finite approximations, algorithms for automata with finite acceptance condition would suffice to solve problems for intuitionistically closed regular languages. In this section, we carry out the plan and obtain efficient automated compositional reasoning for intuitionistically closed regular languages.

Firstly, it is not hard to show the language containment problem for intuitionistically closed regular languages is equivalent to those for regular languages. Intuitively, if all finite approximations of an intuitionistically closed regular language are contained in another intuitionistically closed regular language, their completions belong to the latter as well.

Lemma 5. *Let R and S be Landweber automata. $L_*(R) \subseteq L_*(S)$ if and only if $L_\infty(R) \subseteq L_\infty(S)$.*

Next, we show that it is possible to deduce information about intuitionistically closed regular languages from their finite approximations.

Theorem 4. *Let $R, S,$ and T be Landweber automata. Then $L_*(R) \odot L_*(S) \subseteq L_*(T)$ if and only if $L_\infty(R) \odot L_\infty(S) \subseteq L_\infty(T)$, where $\odot \in \{\cup, \cap, \rightarrow\}$.*

Consider the compositional proof rules *R0* in Section 3, both premises are equivalent to the regular language containment problem by Theorem 4. That is, for any Landweber automata M_0, M_1, and P, we have

$$\text{R0'}\ \frac{L_*(M_0) \cap L_*(A) \subseteq L_*(P) \qquad L_*(M_1) \subseteq L_*(A)}{L_\infty(M_0) \cap L_\infty(M_1) \subseteq L_\infty(P)}$$

Since the premises $L_*(M_0) \cap L_*(A) \subseteq L_*(P)$ and $L_*(M_1) \subseteq L_*(A)$ are instances of the regular language containment problem, learning algorithms for regular languages suffice to generate the weakest assumption in the new rule. The most efficient learning algorithm for regular languages requires $O(kmn^2)$ and $n-1$ membership and equivalence queries respectively, where k is the size of alphabet, n is the number of states, and m is the length of the longest counterexample [13]. In comparison, the most efficient learning algorithm for any subclass of ω-regular languages requires $O(n^4)$ and $O(n^2)$ membership and equivalence queries respectively [12]. Since it is harder to resolve the containment problem for ω-regular languages, the compositional proof rule (R0') is definitely preferred.

8 Conclusion

The class of intuitionistically closed regular languages was introduced. We showed that the class forms a Heyting algebra and is finitely approximatable. It moreover admits circular compositional proof rules. Our results extend automated compositional reasoning to the class of intuitionistically closed regular languages most satisfactorily. Not only can compositional proof rules for the new class be deduced automatically, but also finding assumptions be done as efficiently as for regular languages. Given the negative result on classically closed ω-regular languages (Section 3), the present work is perhaps the best that one can hope for the compositional analysis of safety properties.

Our interpretation for intuitionistic languages differs from those in [11]. It would be interesting to investigate more properties about intuitionistic regular languages in our interpretation. Moreover, a correspondence between intuitionistic languages and automata in the interpretation of [11] could be useful to solve the model checking problem of intuitionistic linear temporal logic.

References

1. Abadi, M., Plotkin, G.D.: A logical view of composition. Theoretical Computer Science **114**(1) (1993) 3–30
2. Alpern, B., Schneider, F.: Defining liveness. Information Processing Letters **21** (1985) 181–185
3. Alur, R., Henzinger, T.: Reactive modules. Formal Methods in System Design **15**(1) (1999) 7–48
4. Angluin, D.: Learning regular sets from queries and counterexamples. Information and Computation **75**(2) (1987) 87–106
5. Barringer, H., Giannakopoulou, D., Păsăreanu, C.S.: Proof rules for automated compositional verification through learning. In: Workshop on Specification and Verification of Component-Based Systems. (2003) 14–21
6. Cobleigh, J.M., Giannakopoulou, D., Păsăreanu, C.S.: Learning assumptions for compositional verification. In Garavel, H., Hatcliff, J., eds.: TACAS. Volume 2619 of LNCS., Springer-Verlag (2003) 331–346
7. de Roever, W.P., de Boer, F., Hanneman, U., Hooman, J., Lakhnech, Y., Poel, M., Zwiers, J.: Concurrency Verification: Introduction to Compositional and Non-compositional Methods. Number 54 in Cambridge Tracts in Theoretical Computer Science. Cambridge University Press (2001)
8. Farzan, A., Chen, Y.F., Clarke, E.M., Tsay, Y.K., Wang, B.Y.: Extending automated compositional verification to the full class of omega-regular languages. In Ramakrishnan, C., Rehof, J., eds.: TACAS. Volume 4963 of LNCS., Springer-Verlag (2008) 2–17
9. Goldblatt, R.: Topoi: The Categorial Analysis of Logic. revised edn. Dover Publications (2006)
10. Landweber, L.: Decision problems for ω-automata. Mathematical Systems Theory **3** (1969) 376–384
11. Maier, P.: Intuitionistic LTL and a new characterization of safety and liveness. In Marcinkowski, J., Tarlecki, A., eds.: Computer Science Logic. Volume 3210 of LNCS., Springer-Verlag (2004) 295–309
12. Maler, O., Pnueli, A.: On the learnability of infinitary regular sets. Information and Computation **118**(2) (1995) 316–326
13. Rivest, R.L., Schapire, R.E.: Inference of finite automata using homing sequences. Information and Computation **103**(2) (1993) 299–347
14. Staiger, L.: ω-languages. In Rozenberg, G., Salomaa, A., eds.: Handbook of Formal Languages. Volume 3. Springer-Verlag (1997) 339–387
15. Thomas, W.: Automata on infinite objects. In van Leeuwen, J., ed.: Handbook of Theoretical Computer Science. Volume B. Elsevier Science Publishers (1990) 133–191
16. Vardi, M.: Verification of concurrent programs: the automata-theoretic framework. In: Proceedings of the Second IEEE Symposium on Logic in Computer Science. (1987) 167–176
17. Wagner, K.: On ω-regular sets. Information and Control **43** (1979) 123–177
18. Wang, B.Y.: Automatic derivation of compositional rules in automated compositional reasoning. In Caires, L., Vasconcelos, V.T., eds.: CONCUR. Volume 4703 of LNCS., Springer-Verlag (2007) 303–316