The Algebra of Iterative Constructions

Kevin Batz
kevin.batz@cs.rwth-aachen.de
Cornell University
Ithaca, United States

Benjamin Lucien Kaminski
kaminski@cs.uni-saarland.de
Saarland University,
Saarland Informatics Campus
Saarbrücken, Germany
University College London
London, United Kingdom

Lucas Kehrer
kehrer@cs.uni-saarland.de
Saarland University,
Saarland Informatics Campus
Saarbrücken, Germany

Gerwin Klein
gerwin.klein@proofcraft.systems
Proofcraft
University of New South Wales
Sydney, Australia

Henning Urbat
henning.urbat@fau.de
Friedrich-Alexander-Universität
Erlangen-Nürnberg
Nürnberg, Germany

Todd Schmid
t.schmid@bucknell.edu
Bucknell University
Lewisburg, Pennsylvania, USA

Abstract

Fixed points are a recurring theme in computer science and are often constructed as limits of suitably seeded fixed point iterations. We present the *algebra of iterative constructions* (AIC) – a purely algebraic approach to reasoning about fixed point iterations of continuous endomaps on complete lattices. AIC allows derivations of constructive fixed point theorems via equational logic and avoids explicit computations with indices. We demonstrate the applicability of AIC by providing algebraic proofs of several well- and less-well-known fixed point theorems: Among others, we prove the *Tarski-Kantorovich principle* – a generalization of the *Kleene fixed point theorem* – as well as a fixed point-theoretic generalization of k-induction, which is used in software verification.

We moreover improve upon a recent generalization of the Tarski-Kantorovich principle due to Olszewski for obtaining pre- and post-fixed points from lattice-theoretic limit inferiors and limit superiors trough iterating an endomap on an *arbitrary* seed element: We identify sufficient continuity conditions on the endomaps so that these limits become *proper* fixed points.

We have mechanized our algebra in Isabelle/HOL. Isabelle's sledgehammer tool is able to find proofs of the above fixed point theorems fully automatically.

Finally, we investigate the completeness of our axiomatization of AIC. We prove that our finite set of finitary axioms is (a) sound but incomplete for standard models of AIC (sequences of elements from a complete lattice) and that (b) a different finite set of *infinitary* axioms is complete. We also prove that infinitary axioms are *unavoidable*: there exists no complete axiomatization of standard models given by *finitely many finitary* axioms.

LICS '26, Lisbon, Portugal

ACM ISBN 978-1-4503-XXXX-X/2018/06
https://doi.org/XXXXXXX.XXXXXXX

CCS Concepts

• **Do Not Use This Code → Generate the Correct Terms for Your Paper**; *Generate the Correct Terms for Your Paper*; Generate the Correct Terms for Your Paper; Generate the Correct Terms for Your Paper.

ACM Reference Format:
Kevin Batz, Benjamin Lucien Kaminski, Lucas Kehrer, Gerwin Klein, Henning Urbat, and Todd Schmid. 2018. The Algebra of Iterative Constructions. In *Proceedings of Logic in Computer Science (LICS '26)*. ACM, New York, NY, USA, 42 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction and Overview

Fixed points are ubiquitous in computer science and related fields: shortest paths [24], game equilibria [25], social choice theory [12], dynamical systems [15], or semantics [1, 13] and verification [9] are only a few of many instances.

In verification, for example, a common task is to approximate the greatest fixed point (gfp) of a continuous endomap F from below, because this amounts to finding a loop invariant that implies the most general loop invariant. Let a be a *candidate* for such a lower bound on gfp F. Then if $a \preceq F(a)$ holds, we have – by coinduction – verified that the candidate a *is indeed* a lower bound on gfp F. Dually, if $F(a) \preceq a$, then a is a verified *upper bound* on lfp F, so:

$$a \preceq F(a) \quad \text{implies} \quad a \preceq \operatorname{gfp} F\,, \qquad \text{and}$$
$$F(a) \preceq a \quad \text{implies} \quad \operatorname{lfp} F \preceq a\,.$$

One justification of the above goes through a certain *fixed point iteration* principle: Consider the case for gfp F. If $a \preceq F(a)$, then this "kicks off" an ascending fixed point iteration $a \preceq F(a) \preceq F^2(a) \preceq \dots$ which (under suitable continuity conditions on F) in the limit (supremum) converges to a fixed point "just above" a. More precisely: $\sup_{k\in\omega} F^k(a)$ is the least fixed point of F that is greater than or equal to a. Since $a \preceq \sup_{k\in\omega} F^k(a)$ and since $\sup_{k\in\omega} F^k(a)$ is itself a fixed point and is hence necessarily less or equal to the *greatest* fixed point gfp F, we get that $a \preceq \operatorname{gfp} F$. Dually, if $F(a) \preceq a$, then $\inf_{k\in\omega} F^k(a)$ is the *greatest* fixed point of F "just below" a and a upper-bounds lfp F. This fixed point iteration principle is called the *Tarski-Kantorovich principle* [16].

But what if neither $a \preceq F(a)$ nor $F(a) \preceq a$ hold?

What does iterating F on a yield?

Is $\lim_{k\to\omega} F^k(a)$ even well-defined? Indeed, both $\liminf_{k\to\omega} F^k(a)$ and $\limsup_{k\to\omega} F^k(a)$ are well-defined and (under certain slightly stronger continuity conditions on F) they are both *fixed points* of F. In other words: From *all* candidates a, we can construct by suitable iteration *some* fixed point (possibly even two distinct ones). This is an improvement on a recent (but unfortunately rather unknown) result due to Olszewski [27] and to the best of our knowledge new.

Also new – and our main methodological contribution – is the way in which we prove such fixed point iteration theorems. Let us first take a completely standard definition of a limit superior

$$\limsup_{k\to\omega} F^k(a) \quad = \quad \inf_{0\le n} \sup_{n\le k} F^k(a)\,.$$

There are really three nested *sequences* involved on the right-hand-side: The first sequence is $\big(F^k(a)\big)_{k\in\omega}$, obtained by iterating F on a. The second one is the sequence $\big(\sup_{n\le k} F^{k(a)}\big)_{n\in\omega}$. By making the index k of the first sequence depend on the index n of the second one, we can imagine how "$\sup_{n\le k}$" acts as an operation, transforming the first into the second sequence. The third sequence is, perhaps surprisingly, $\big(\inf_{m\le n}\sup_{n\le k} F^k(a)\big)_{m\in\omega}$, constructed by "$\inf_{m\le n}$" from the second one, making n depend on m. Our desired limit superior is then at index $m=0$.

Reasoning about limit superiors and inferiors naturally involves such interdependent indices. Nevertheless: *Our key observation is that the exact indices do not really matter and are in fact distracting.* We can rather think of the sup, inf, and $F^{(-)}$ as operations – almost modalities – on sequences: We think of inf as $\Box$, of sup as $\Diamond$, and we turn $F^{(-)}$ into a sort of iteration operation F^*. Altogether, we obtain

$$\limsup_{k\to\omega} F^k(a) \quad = \quad \inf_{0\le n}\sup_{n\le k} F^k(a) \quad \text{“=”} \quad \Box\Diamond F^* a\,.$$

In this paper, we will make the above ideas rigorous and introduce the *algebra of iterative constructions* (AIC), in which we can reason algebraically about fixed points of endomaps on complete lattices. For example, we will be able to prove that for continuous F,

$$F\Diamond F^*\bot \;=\; \Diamond F^*\bot\,,$$

(cf. $\sup_k F^k(\bot)$), thus proving part of the Kleene fixed point theorem. We demonstrate the usefulness of AIC by means of several case studies. Purely within AICs (or to put it a bit flippantly, purely by pushing boxes and diamonds around), we prove:

(1) The Tarski-Kantorovich principle, a generalized version of the well-known Kleene fixed point theorem: If F is ω-continuous, then $\Diamond F^* a$ is the least fixed point of F just above a.

(2) A generalization of Park induction ($a \preceq F(a)$ implies $\mathsf{lfp}\, F \preceq a$), a heavily used principle in verification of various types of systems.

(3) A new improvement on a theorem due to Olszewski [27]: If F is countably continuous (preserving suprema of *arbitrary countable sets*) and ω-cocontinous, $\Box\Diamond F^* a$ is a fixed point of F.

(4) Latticed k-induction [5], a generalization of k-induction [31] that is extremely effective in hardware and software verification.

We have mechanized AIC and the algebraic proofs of the theorems above in Isabelle/HOL. The mechanized algebraic proofs follow the manual exposition closely, with intermediate steps solved automatically. High-level theorems such as Tarski-Kantorovich or Park induction can even be proved fully automatically.

Overview and Organization of the Paper. We present the algebraic structures we treat in this paper – in particular, our standard models, which we call *sequence algebras* – in Section 2. There, we also show how equational proofs for such structures work.

In Section 3, we present a finitary base axiomatization of AIC called AIC_0, which is sound for sequence algebras. We also provide an axiomatization with additional (redundant) axioms called AIC_1, which is more usable for automatic proof search. We demonstrate applicability of AIC through algebraic proofs of fixed point theorems in Section 4.

We comment on the mechanization of AIC in Isabelle/HOL in Section 5. We investigate aspects of (in)completeness of AIC axiomatizations in Section 6. We discuss limitations and give an outlook on future directions in Section 7.

Related Work. *Axiomatic approaches* to fixed point theory have a long tradition in theoretical computer science, having appeared in different settings and levels of generality. The most prominent examples are Kozen's complete axiomatization of the modal μ-calculus [20, 34], and the abstract perspective on fixed point equations of Bloom and Esik's iteration theories [2, 8], which extend the categorical account of universal algebra based on Lawvere theories. While these works are aimed at axiomatically capturing *properties* of least or greatest fixed points, the focus of AIC lies on reasoning about the iterative *construction* of (not necessarily least or greatest) fixed points and related objects, such as pre- and post-fixed points.

Approximating (instead of merely stating the existence of) fixed points was somewhat recently investigated in a series of papers [3, 4, 19]. In particular [3] tackles the problem of approximating in the directions that are *not* covered by usual (co)induction: *under*approximating *least* and *over*approximating *greatest* fixed points.

Finally, our $\Diamond$ operations seem very related to the notion of *least decreasing majorants* from Banach function spaces [18, 30, 32]. We discuss further related work in Section 7.

2 The Algebra of Iterative Constructions

The *algebra of iterative constructions* (AIC) is an *algebraic* theory, in the sense that it comprises an *algebraic signature* that dictates the available operations and their arities, and a set of equational inference rules that tell us how these operations interact with one another. We parameterize the theory in a set $\mathsf{Funcs} = \{F, G, H, \dots\}$ of *function symbols*, which abstractly represent monotonic maps for which we will be constructing and reasoning about fixed points.

Let us first deal with the signature. Given Funcs, the *signature of AIC* consists of two constants $\bot$ and $\top$, two binary operations $\curlyvee$ and $\curlywedge$, four unary operations $\Diamond$, $\Box$, $\circledcirc$, and $\bigcirc$, as well as for each functions symbol $F \in \mathsf{Funcs}$ two unary operations F and F^*. Models of AIC will be *(algebraic) structures* with this signature.

Definition 1 (AIC-Structures). An *AIC-structure* is a tuple

$$\mathcal{A} \;=\; \big(A,\, \bot^{\mathcal{A}},\, \top^{\mathcal{A}},\, \curlyvee^{\mathcal{A}},\, \curlywedge^{\mathcal{A}},\, \Diamond^{\mathcal{A}},\, \Box^{\mathcal{A}},\, \circledcirc^{\mathcal{A}},\, \bigcirc^{\mathcal{A}},\; \{\, F^{\mathcal{A}} \mid F \in \mathsf{Funcs}\,\},\, \{\, F^{*\mathcal{A}} \mid F \in \mathsf{Funcs}\,\}\big)\,,$$

where A is a set with $\bot^{\mathcal{A}}, \top^{\mathcal{A}} \in A$ and $\curlyvee^{\mathcal{A}}, \curlywedge^{\mathcal{A}}\colon A\times A \to A$ and $\Diamond^{\mathcal{A}}, \Box^{\mathcal{A}}, \circledcirc^{\mathcal{A}}, \bigcirc^{\mathcal{A}}, F^{\mathcal{A}}, F^{*\mathcal{A}}\colon A \to A$. The set A is called the *carrier* of $\mathcal{A}$ and we also say that A *carries* $\mathcal{A}$.

Table 1: Overview of metavariables.

$a, b, c, \ldots$	variables (appearing in terms)
$\mathcal{A}, \mathcal{B}, \mathcal{T}, \ldots$	algebraic structures / AIC-structures
$F, G, H, \ldots$	function symbols representing monotonic maps
$\mathfrak{I}$	interpretation of variables (appearing in terms)
$\mathfrak{I}_0$	interpretation of the function symbols
$\ell, m, \cdots$	elements from the ambient lattice
$\varphi, \psi, \vartheta, \ldots$	sequences of lattice elements
$s, t, u, e, \ldots$	iterative construction terms (denoting sequences)

Given two AIC-structures $\mathcal{A}$ and $\mathcal{B}$, an *algebra homomorphism* $h\colon \mathcal{A} \to \mathcal{B}$ is a function $h\colon A \to B$ that preserves the algebraic structure. i.e. $h(\bot^{\mathcal{A}}) = \bot^{\mathcal{B}}$ and $h(\top^{\mathcal{A}}) = \top^{\mathcal{B}}$, and for any $\ell, m \in A$, $h(\ell \vee^{\mathcal{A}} m) = h(\ell) \vee^{\mathcal{B}} h(m)$, and $h(\diamond^{\mathcal{A}} \ell) = \diamond^{\mathcal{B}} h(\ell)$, and so on. ◁

We drop the superscript $^{\mathcal{A}}$ when the $\mathcal{A}$ is clear. An overview of the metavariables we use throughout this paper is given in Table 1.

So far, nothing in the definition of AIC-structures dictates what the different operations mean or how they interact. Since our central aim is to capture iterative constructions of lattice fixed points, we are naturally going to concern ourselves with AIC-structures that are carried by sequences of elements from a lattice.

2.1 Sequence Algebras

Let $\omega = \{0, 1, 2, 3, \ldots\}$ be the natural numbers. Given a set L, a function $\varphi\colon \omega \to L$ is called a *sequence (in L)*. We let L^ω be the *set of all sequences in L*. We usually write $\varphi = \varphi_0\ \varphi_1\ \varphi_2\ \varphi_3 \ldots$, where φ_i denotes the i^{th} element of φ. We say that a sequence is *flat* if it is a *constant* sequence $\ell\ \ell\ \ell\ \ell \ldots$ and denote such a sequence by $\overline{\ell}$.

For the remainder of the paper, $(L, \sqsubseteq)$ is a fixed *countably complete* lattice (i.e. every countable subset $S \subseteq L$, including the empty set, has a supremum and infimum in L) with bottom and top elements $\bot^L$ and $\top^L$, and join and meet denoted by $\sqcup$ and $\sqcap$. We denote by $\mathsf{MonoMaps}(L)$ the set of monotonic maps $L \to L$ (monotonic with respect to $\sqsubseteq$). An example of a countably-complete lattice is the extended real numbers $\overline{\mathbb{R}} = (\mathbb{R} \cup \{-\infty, +\infty\}, \leq)$, for which $\mathsf{MonoMaps}(\overline{\mathbb{R}})$ consists of the nondecreasing functions.

We will now define the kind of AIC-structures suitable for reasoning about fixed point iterations of monotonic endomaps in L.

Definition 2 (Sequence Algebras). Every countably complete lattice $(L, \sqsubseteq)$ together with an *interpretation of the function symbols* $\mathfrak{I}_0\colon \mathsf{Funcs} \to \mathsf{MonoMaps}(L)$ induces an AIC-structure carried by L^ω with the following operations: for any $\varphi, \vartheta \in L^\omega$ and $n \in \omega$,

$$\bot_n = \bot^L \qquad \top_n = \top^L \tag{2.1}$$

$$(\varphi \vee \vartheta)_n = \varphi_n \sqcup \vartheta_n \qquad (\varphi \wedge \vartheta)_n = \varphi_n \sqcap \vartheta_n \tag{2.2}$$

$$(\circledcirc\, \varphi)_n = \varphi_0 \qquad (\bigcirc\, \varphi)_n = \varphi_{n+1} \tag{2.3}$$

$$(\diamond\, \varphi)_n = \sup_{k \geq n} \varphi_k \qquad (\square\, \varphi)_n = \inf_{k \geq n} \varphi_k \tag{2.4}$$

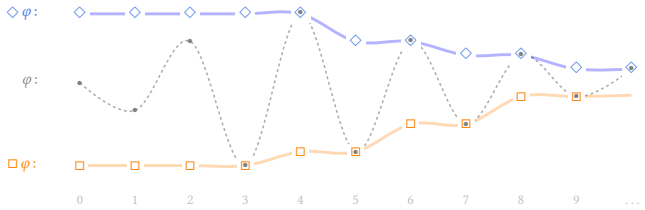
$$(F\, \varphi)_n = \mathfrak{I}_0(F)(\varphi_n) \qquad (F^*\varphi)_n = \mathfrak{I}_0(F)^n(\varphi_n) \tag{2.5}$$

An AIC-structure of this kind is called a *sequence algebra.* ◁

To capture fixed point iterations, all members of a sequence algebra are sequences. As we will demonstrate in Section 4, the constants and algebraic operations that make up sequence algebras are ubiquitous in lattice fixed point (iteration) theorems. Lines (2.1–2.2) lift the constants and operations from the underlying lattice pointwise to sequences: the constants $\bot$ and $\top$ are the *flat* sequences $\bot^L\ \bot^L\ \bot^L\ \bot^L \ldots \in L^\omega$ and $\top^L\ \top^L\ \top^L\ \top^L \ldots \in L^\omega$. The operation $\vee$ takes two sequences φ and ϑ and yields their element-wise join $\varphi_0 \sqcup \vartheta_0\ \ \varphi_1 \sqcup \vartheta_1\ \ \varphi_2 \sqcup \vartheta_2\ \ \ldots$; dually, $\wedge$ is the element-wise meet.

The two operations on Line (2.3) are called *head* and *shift*. The *head* operation $\circledcirc$ takes a sequence $\varphi = \varphi_0\ \varphi_1\ \varphi_2\ \varphi_3 \ldots$ and yields a flat repetition of φ's 0^{th} element, i.e. $\varphi_0\ \varphi_0\ \varphi_0\ \varphi_0 \ldots$. The *shift* operation $\bigcirc$ shifts sequences by one position to the left (while deleting the 0^{th} element). Together, $\circledcirc$ and $\bigcirc$ allow extracting single sequence elements in the following sense: identifying a lattice element $\ell \in L$ with its corresponding flat sequence $\ell\ \ell\ \ell\ \ell \ldots \in L^\omega$, the k^{th} element of a sequence φ can be expressed as $\circledcirc \bigcirc^k \varphi = \circledcirc \bigcirc \overset{k \text{ times}}{\cdots} \bigcirc\, \varphi$.

The operations on Line (2.4) are called *majorum* and *minorum*, respectively. For the majorum $\diamond\, \varphi$, the element at index n is the supremum of all (countably many) elements of φ with index $\geq n$. It is clear that $\diamond\, \varphi$ is a *majorant* of φ, i.e., $\varphi_n \sqsubseteq (\diamond\, \varphi)_n$ for all n. Moreover, the sequence $\diamond\, \varphi$ always *descends*: For instance, the supremum at index 0 can "see" all elements of φ, whereas at index 1 it can "see" all but the 0^{th} element. Hence, the latter can only ever yield a potentially smaller supremum. In fact, $\diamond\, \varphi$ is the *least decreasing majorant of φ*. Similar concepts have been studied for Banach function spaces also under the name *least decreasing majorant* or *essential supremum* [18, 30, 32]. Dually, for the minorum $\square\, \varphi$, the n^{th} element is the infimum of all elements with index $\geq n$. $\square\, \varphi$ is a *minorant* of φ, i.e. $(\square\, \varphi)_n \sqsubseteq \varphi_n$ and it is the *greatest increasing minorant of φ*. A depiction of $\diamond\, \varphi$ and $\square\, \varphi$ is provided below:



Gray •'s depict elements of φ, blue ◇'s the elements of $\diamond\, \varphi$, and orange □'s the elements of $\square\, \varphi$. Continuous lines connecting elements are for better visualization. All sequences are discrete.

Here, we can see visually that $\diamond\, \varphi$ is a *descending majorant* of φ whereas $\square\, \varphi$ is an *ascending minorant*. We can also see how $\diamond\, \varphi$ and $\square\, \varphi$ together form the *tightest monotonic envelope* around φ. Finally, we reiterate that $\diamond\, \varphi$ and $\square\, \varphi$ are *not* simply the global supremum and infimum of all the elements of φ. Global infimum and supremum of φ are expressible as $\circledcirc\, \square\, \varphi$ and $\circledcirc\, \diamond\, \varphi$, respectively.

The operations in Line (2.5) are the *function application* and *orbit* operations. For simplicity, let us omit $\mathfrak{I}_0$ from the notation and treat F (as opposed to $\mathfrak{I}_0(F)$) as a monotonic endomap on L. Then $F\, \varphi$ is the element-wise application of F to φ, i.e. it yields the sequence[1]

$$F\, \varphi \quad = \quad F(\varphi_0)\ \ F(\varphi_1)\ \ F(\varphi_2)\ \ F(\varphi_3) \ldots\ .$$

The unary operation F^* yields the *iteration* of F on a lattice element. However, the input to F^* is already a sequence and so we need F^* to operate on sequences. For this, we apply F zero times to the 0^{th}

[1] More accurately, the sequence $\mathfrak{I}_0(F)(\varphi_0)\ \ \mathfrak{I}_0(F)(\varphi_1)\ \ \mathfrak{I}_0(F)(\varphi_2)\ \ \mathfrak{I}_0(F)(\varphi_3) \ldots$.

element of φ, once to the 1st element, twice to the 2nd element, and so forth, thus yielding the sequence

$$F^*\varphi \quad = \quad \varphi_0 \;\; F(\varphi_1) \;\; F^2(\varphi_2) \;\; F^3(\varphi_3) \dots \; .$$

When we apply F^* to a flat sequence $\overline{\ell} = \ell\,\ell\,\ell\,\ell\dots$ then $F^*\overline{\ell}$ is indeed the *F-orbit* of $\ell \in L$, i.e. the sequence $F^*\overline{\ell} \;=\; \ell \;\; F(\ell) \;\; F^2(\ell) \;\; F^3(\ell) \dots$.

2.2 Iterative Construction Terms

Sequence algebras are where iterative constructions of lattice fixed points live. By combining the operations of a sequence algebra, one can obtain a variety of different recipes for constructing fixed points. In fact, we will see in Section 4 that many fixed point constructions can be carried out using $\Diamond$, $\Box$, and F^* alone. For example, the least fixed point of F can (under certain continuity assumptions on F) be expressed as $\Diamond F^*\bot$, which should look familiar when recalling the construction from the Kleene fixed point theorem (i.e. $\sup_n F^n(\bot)$).

Our ultimate goal is to be able to algebraically manipulate these different recipes for constructing lattice fixed points and thereby carry out algebraic proofs of fixed point theorems. This requires a syntax for writing these recipes down, as well as a set of inference rules with which we can prove identities and other algebraic laws.

Definition 3 (Syntax of Iterative Construction Terms). For a fixed set $\mathsf{Vars} = \{a, b, \dots\}$ of *variables*, the set Terms of *iterative construction terms* (or simply, *terms*), ranging over metavariables $s, t, \dots$, adheres to the grammar below, where $a \in \mathsf{Vars}$ and $F \in \mathsf{Funcs}$:[2]

$$s \;\longrightarrow\; \bot \mid \top \mid a \mid s \vee s \mid s \wedge s \mid \circledcirc s \mid \bigcirc s \mid \Diamond s \mid \Box s \mid F s \mid F^* s \qquad \triangleleft$$

Every term s represents a recipe for constructing new sequences from known ones. The known sequences can well be left arbitrary/uninterpreted and terms hence feature variables $a, b, c, \dots$ which have to be interpreted to obtain a concrete sequence.

Definition 4 (Interpretations). Given an AIC-structure $\mathcal{A}$ carried by A, an *interpretation* (in $\mathcal{A}$) is a function $\mathfrak{I}\colon \mathsf{Vars} \to \mathcal{A}$ that maps variables to elements of A. We say that $\mathfrak{I}$ is a *standard interpretation* if $\mathcal{A}$ is a sequence algebra. $\triangleleft$

Given a sequence algebra $\mathcal{A}$ carried by L^ω and a standard interpretation $\mathfrak{I}\colon \mathsf{Vars} \to L^\omega$, each term s denotes the sequence obtained by recursively evaluating its operations after replacing each occurrence of a variable a in s with $\mathfrak{I}(a)$. Formally, the set Terms of iterative construction terms itself carries an AIC-structure called the *term algebra* $\mathcal{T}$, whose operations are given by term formation (e.g. $\bigcirc^{\mathcal{T}} a = \bigcirc a$), and every interpretation $\mathfrak{I}\colon \mathsf{Vars} \to \mathcal{A}$ extends to a unique algebra homomorphism ${}^{\mathfrak{I}}[\![-]\!]\colon \mathcal{T} \to \mathcal{A}$. For instance, ${}^{\mathfrak{I}}[\![\bigcirc a]\!] = {}^{\mathfrak{I}}[\![\bigcirc^{\mathcal{T}} a]\!] = \bigcirc^{\mathcal{A}} {}^{\mathfrak{I}}[\![a]\!] = \bigcirc^{\mathcal{A}} \mathfrak{I}(a)$. This unique homomorphism yields the semantics of terms under a given interpretation.

Definition 5 (Semantics of Terms). Let $\mathcal{A}$ be an AIC-structure, let $\mathfrak{I}$ be an interpretation in $\mathcal{A}$, and let ${}^{\mathfrak{I}}[\![-]\!]\colon \mathcal{T} \to \mathcal{A}$ be the unique algebra homomorphism satisfying ${}^{\mathfrak{I}}[\![a]\!] = \mathfrak{I}(a)$ for every $a \in \mathsf{Vars}$. Then for each term $s \in \mathsf{Terms}$, we call ${}^{\mathfrak{I}}[\![s]\!]$ the *$\mathfrak{I}$-semantics* of s. $\triangleleft$

While Definitions 4 and 5 allow interpretations (and hence semantics) in arbitrary AIC-structures, we are primarily trying to capture the sequence algebras. Hence, we call interpretations in sequence algebras *standard interpretations*. We record the semantics of iterative construction terms under a standard interpretation in Table 2.

As we will see, standard interpretations capture many important aspects of iterative fixed point constructions.

Remark 1 (On Interpretations of Variables and Functions). We typically bundle the interpretation of the function symbols $\mathfrak{I}_0$ in with the standard interpretation, and simply write $\mathfrak{I}(F)$ instead of $\mathfrak{I}_0(F)$ for each $F \in \mathsf{Funcs}$. While an abuse of notation, we could have equivalently defined a standard interpretation to be a suitable function $\mathfrak{I}\colon \mathsf{Vars} \cup \mathsf{Funcs} \to L^\omega \cup \mathsf{MonoMaps}(L)$. $\triangleleft$

2.3 Quasiequations

For two terms s and t, we call a formal expression $s = t$ an *identity*. For instance, $F\,a = a$ is an identity (expressing that a is a fixed point of F).[3] Fixed point theorems usually require certain assumptions, so that a is indeed a fixed point. We therefore want to be able to derive identities that hold, provided that other identities (the assumptions) hold. This is captured by *quasiequations* (a.k.a. *quasi-identities*).

Definition 6 (Quasiequations, Axiom Systems). A *quasiequation* Q is a formula of the form

$$\big(\textstyle\bigwedge_{i\in I} {}^i s \;=\; {}^i t\big) \quad\Longrightarrow\quad s \;=\; t \qquad (\mathrm{Q})$$

for some index set I and iterative construction terms $s, t, {}^i s, {}^i t \in \mathsf{Terms}$, for each $i \in I$. The identities ${}^i s = {}^i t$ are called the *premises* and $s = t$ is called the *conclusion* of Q. The quasiequation Q is called *finitary* if it has only finitely many premises (i.e. if I is finite).

An AIC-structure $\mathcal{A}$ carried by A *satisfies* Q, denoted $\mathcal{A} \models \mathrm{Q}$, if for any interpretation $\mathfrak{I}\colon \mathsf{Vars} \to A$ the following holds:

$$\text{if} \quad \text{for all } i \in I\colon {}^{\mathfrak{I}}[\![{}^i s]\!] \;=\; {}^{\mathfrak{I}}[\![{}^i t]\!] \quad \text{then} \quad {}^{\mathfrak{I}}[\![s]\!] \;=\; {}^{\mathfrak{I}}[\![t]\!].$$

A quasiequation is *valid (for sequence algebras)* if it is satisfied by every sequence algebra.

An *axiom system* Ax is a set of quasiequations and its elements are called the *axioms* (of Ax). We say that Ax is *finite* if it is a finite set, and *finitary* if all axioms are finitary. An AIC-structure $\mathcal{A}$ *satisfies* Ax, written $\mathcal{A} \models \mathsf{Ax}$, if $\mathcal{A} \models \mathrm{Q}$ for every $\mathrm{Q} \in \mathsf{Ax}$. In this case, $\mathcal{A}$ is a *model* of Ax. An axiom system Ax is *sound (for sequence algebras)* if every axiom is valid for sequence algebras.

We generally prefer to write quasiequations like Q from Definition 6 as inference rules of the form

$$\frac{{}^1 s \;=\; {}^1 t \qquad {}^2 s \;=\; {}^2 t \qquad \cdots}{s \;=\; t}\;\mathrm{Q} \qquad \text{or} \qquad \frac{\mathrm{Q}}{s \;=\; t}$$

where $I = \{1, 2, \dots\}$ in case of the left inference rule and $I = \emptyset$ in case of the right one. For $I = \emptyset$, the notion of quasiequation and identity collapse into a single notion and so we can also speak of satisfaction and validity of identities.

Quasiequations are, in a formal sense [21], *algebraic* laws, which means that satisfaction is preserved by substitution: Let $s, e \in \mathsf{Terms}$, $a \in \mathsf{Vars}$, and let $s\,[a \backslash e]$ be the term obtained by replacing each occurrence of a in s with e. Then algebraicity means that if $\mathcal{A} \models (\bigwedge_{i\in I} {}^i s = {}^i t) \Longrightarrow s = t$, then we also know that

[2] Parenthesizing is handled in the usual manner: unary symbols ($\bigcirc, \Diamond, \dots$) bind stronger than binary ones ($\vee$, $\wedge$), and unary symbols associate to the right, e.g. $\Diamond F s = \Diamond (F s)$.

[3] More precisely, interpreted in a sequence algebra, this states that a_n is a fixed point of F for all $n \in \omega$. This is because $F\,a$ is F applied pointwise to a.

Table 2: Semantics of iterative construction terms under a standard interpretation $\mathfrak{I}$.

Term c	Semantics ${}^{\mathfrak{I}}[\![c]\!]_n$	Name	Remarks	Intuition
$\bot$	$\bot$	bottom	constant sequence of $\bot^L$'s	$\bot\ \bot\ \bot\ \bot\ldots$
$\top$	$\top$	top	constant sequence of $\top^L$'s	$\top\ \top\ \top\ \top\ldots$
a	$\mathfrak{I}(a)_n$	variable	the *sequence* $\mathfrak{I}(a)$	$a_0\ a_1\ a_2\ a_3\ldots$
$s \curlyvee t$	${}^{\mathfrak{I}}[\![s]\!]_n \sqcup {}^{\mathfrak{I}}[\![t]\!]_n$	join	element-wise join of s and t	$s_0 \curlyvee t_0\ \ s_1 \curlyvee t_1\ \ s_2 \curlyvee t_2\ \ s_3 \curlyvee t_3\ldots$
$s \curlywedge t$	${}^{\mathfrak{I}}[\![s]\!]_n \sqcap {}^{\mathfrak{I}}[\![t]\!]_n$	meet	element-wise meet of s and t	$s_0 \curlywedge t_0\ \ s_1 \curlywedge t_1\ \ s_2 \curlywedge t_2\ \ s_3 \curlywedge t_3\ldots$
$\Diamond s$	$\sup_{n\le k} {}^{\mathfrak{I}}[\![s]\!]_k$	majorum	n^{th} element is the supremum over all elements with index $\ge n$	$\sup_{0\le k} s_k\ \ \sup_{1\le k} s_k\ \ \sup_{2\le k} s_k\ \ \sup_{3\le k} s_k\ldots$
$\Box s$	$\inf_{n\le k} {}^{\mathfrak{I}}[\![s]\!]_k$	minorum	n^{th} element is the infimum over all elements with index $\ge n$	$\inf_{0\le k} s_k\ \ \inf_{1\le k} s_k\ \ \inf_{2\le k} s_k\ \ \inf_{3\le k} s_k\ldots$
$\circledcirc s$	${}^{\mathfrak{I}}[\![s]\!]_0$	head	repeat 0^{th} element	$s_0\ s_0\ s_0\ s_0\ldots$
$\bigcirc s$	${}^{\mathfrak{I}}[\![s]\!]_{n+1}$	shift	drop 0^{th} element and left-shift all other elements by 1 index	$s_1\ s_2\ s_3\ s_4\ldots$
$F s$	$\mathfrak{I}(F)\left({}^{\mathfrak{I}}[\![s]\!]_n\right)$	function application	apply $\mathfrak{I}(F)$ element-wise to s	$F(s_0)\ \ F(s_1)\ \ F(s_2)\ \ F(s_3)\ldots$
$F^* s$	$\mathfrak{I}(F)^n\left({}^{\mathfrak{I}}[\![s]\!]_n\right)$	orbit	n^{th} element is the n-fold iteration of $\mathfrak{I}(F)$ on the n^{th} element of s	$s_0\ \ F(s_1)\ \ F^2(s_2)\ \ F^3(s_3)\ldots$

$$\frac{}{a = a}\ \text{EQ-REFLEX} \qquad \frac{a = b}{b = a}\ \text{SYMM} \qquad \frac{a = b \qquad b = c}{a = c}\ \text{EQ-TRANS}$$

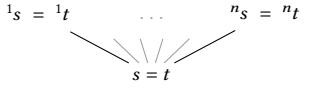
$$\frac{{}^1a = {}^1b \qquad \cdots \qquad {}^na = {}^nb}{\circledast\left({}^1a, \ldots, {}^na\right) = \circledast\left({}^1b, \ldots, {}^nb\right)}\ \text{CONG}$$

Figure 1: The inference rules of equational logic. Above, $a, b, {}^ia, {}^ib, c \in$ Vars, $\circledast$ ranges over the operations of arity $n > 0$ appearing in the signature of the algebra under consideration. In our case $\circledast \in \{\curlyvee, \curlywedge, \circledcirc, \bigcirc, \Diamond, \ldots\}$, so $n \in \{1, 2\}$.

$\mathcal{A} \models (\bigwedge_{i\in I} {}^is\,[a\backslash e] = {}^it\,[a\backslash e]) \Longrightarrow s\,[a\backslash e] = t\,[a\backslash e]$. The latter quasiequation is a *substitution instance* of the former. Substitution instances of quasiequations can be obtained from any substitution of variables with terms: given a mapping $\sigma\colon$ Vars $\to$ Terms and a term s, we write $s[\sigma]$ for the term obtained by simultaneously substituting each variable a in term s with term $\sigma(a)$.[4]

Quasiequational logic lets us derive new quasiequations syntactically from known ones using *derivations*, which are a form of inference tree in the following sense: a *(finite) inference tree* is a (finite) tree whose nodes are labelled with identities (i.e. expressions of the form $s = t$ for two terms s and t). In an inference tree, points of branching are interpreted as inference rules:

$$\frac{{}^1s = {}^1t \qquad \cdots \qquad {}^ns = {}^nt}{s = t} \qquad \text{“=”}$$



Definition 7 (Derivations and Provability). Let Ax be an axiom system, and let $\mathfrak{Q}$ be a finitary quasiequation. A *derivation of* $\mathfrak{Q}$ *from* Ax is a finite inference tree such that the root is labelled with the conclusion of $\mathfrak{Q}$, and moreover every node is either (i) a leaf labelled with some premise of $\mathfrak{Q}$, or (ii) a point of branching of the form

$$\frac{{}^1s[\sigma] = {}^1t[\sigma] \qquad \cdots \qquad {}^ns[\sigma] = {}^nt[\sigma]}{s[\sigma] = t[\sigma]}$$

for some quasiequation $(\bigwedge_{i=1}^n {}^is = {}^it) \Longrightarrow s = t$ in Ax or in equational logic (see Figure 1), and some substitution $\sigma\colon$ Vars $\to$ Terms. We say that $\mathfrak{Q}$ is *derivable (*or *provable)* from Ax and write Ax $\vdash \mathfrak{Q}$ if $\mathfrak{Q}$ has a derivation from Ax. ◁

Remark 8. (1) We stress that Definition 7 (ii) may apply to leaves (where $n = 0$); for example any instance of using EQ-REFLEX.

(2) An axiom system Ax is sound for sequence algebras iff all quasiequations derivable from Ax are valid for sequence algebras. This is because our proof system is standard quasiequational logic, which cannot derive non-valid quasiequations from valid ones.

(3) If Ax $\vdash \mathfrak{Q}$, we may add $\mathfrak{Q}$ to Ax without increasing the expressive strength of Ax. Formally, if both Ax $\vdash \mathfrak{Q}$ and Ax $\cup \{\mathfrak{Q}\} \vdash \mathfrak{Q}'$, then already Ax $\vdash \mathfrak{Q}'$. Indeed, whenever we would use $\mathfrak{Q}$ within a derivation of $\mathfrak{Q}'$ from Ax $\cup \{\mathfrak{Q}\}$, we might as well “inline” a derivation of a suitable substitution instance of $\mathfrak{Q}$ from Ax instead. It *can* make a difference for the automation of theorem proving, however, whether $\mathfrak{Q}'$ is present in the axiom system or not, cf. Section 5. ◁

2.4 Quasi-Inequalities

Lattice-theoretic fixed point theorems often refer to the underlying partial order $\sqsubseteq$ of the lattice. For instance, *Park induction* states that $F(\ell) \sqsubseteq \ell$ implies $\mathsf{lfp}\ F \sqsubseteq \ell$. Since $\sqsubseteq$ is so prevalent in lattice-theoretic fixed point theorems, we want to be able to make judgements directly about $\sqsubseteq$, thus rendering theorem statements and proofs more readable and potentially more automatable. Reasoning about $\sqsubseteq$ is not more general than reasoning about $=$, because

[4] In other words, $s[\sigma] = {}^{\sigma}[\![s]\!]$; cf. Section 2.2.

in any lattice $(L, \sqsubseteq)$ with meet $\sqcap$ and join $\sqcup$, and $\ell, m \in L$, we have $\ell \sqsubseteq m$ if and only if $\ell \sqcup m = m$ (or equivalently $\ell = m \sqcap \ell$).

As every sequence algebra is a lattice with meet $\wedge$ and join $\vee$, also here we can recover the underlying partial order via the meet and join operations: $\varphi_n \sqsubseteq \vartheta_n$ for all $n \in \omega$ if and only if $\varphi \vee \vartheta = \vartheta$. This allows us to treat point-wise inequalities between sequences from L, as equations and thus appeal to the correctness of equational logic reasoning.

While the reasoning under the hood is equational, our aim is still to reason about inequalities. We thus introduce the shorthand notation $s \preceq t$ for the identity $s \vee t = t$.

Definition 9 (Quasi-Inequalities). An *inequality* is an identity of the form $s \vee t = t$, denoted $s \preceq t$, for $s, t \in \mathrm{Terms}$. A quasiequation $\left(\bigwedge_{i\in I} {}^i s \preceq {}^i t\right) \Longrightarrow s \preceq t$ is called a *quasi-inequality*. ◁

An inequality $s \preceq t$ is valid for sequence algebras iff for any standard interpretation $\mathfrak{I}$ and any $n \in \omega$, we have ${}^{\mathfrak{I}}[\![s]\!]_n \sqsubseteq {}^{\mathfrak{I}}[\![t]\!]_n$. It is direct from the definition of lattice that $s = t$ is valid if and only if both $s \preceq t$ and $t \preceq s$ are valid. A number of interesting properties of sequences can be expressed as inequalities:

a is an ascending chain	$a \preceq \bigcirc a$
a is a descending chain	$\bigcirc a \preceq a$
a is flat	$\Diamond a \preceq \Box a$
a converges	$\Box\Diamond a \preceq \Diamond\Box a$
all elements of a are prefixed points of F	$F a \preceq a$
all elements of a are postfixed points of F	$a \preceq F a$

3 Axioms for Iterative Constructions

We now present two axiom systems, AIC_0 and AIC_1, for the algebra of iterative constructions. AIC_0 is a *basic* set of axioms that is sound for sequence algebras. It is intended to be small, so that it is easy to prove whether or not some class of structures forms models of AIC.

For more usable, i.e. more readable *and more automatable*, algebraic proofs of lattice-theoretic fixed point theorems, we introduce the extended axiom system AIC_1. All additional axioms in $\mathsf{AIC}_1 \setminus \mathsf{AIC}_0$ are derivable from AIC_0 and hence every model of AIC_0 is also a model of AIC_1. The extended system AIC_1 is indeed more usable: Isabell's sledgehammer tool finds proofs of all fixed point theorems in Section 4 *automatically* in AIC_1 but not in AIC_0.

We stress that AIC_0 is *not complete* for sequence algebras (thus neither is AIC_1), nor can any finite system of finitary axioms achieve completeness, cf. Section 6.1. There is hence no point in attempting to provide a *minimal* finitary axiomatization. A complete but *infinitary* axiomatization of sequence algebras is given in Section 6.2.

3.1 The Basic Axiom System AIC_0

The basic axiom system AIC_0 is shown in Figure 2. Since we want to capture sequence algebras, we provide intuitions for the setting where variables represent *sequences*. However, it should be noted that our axioms do *not* explicitly axiomatize that we are operating on sequences. There could well be other models.

3.1.1 Bounded Lattice and Shifts. These axioms state that models of AIC_0 form a *bounded lattice* with join $\vee$, meet $\wedge$, least element $\bot$ and greatest element $\top$; that shifting is a monotonic operation; and that $\bigcirc$ distributes over $\vee$ and $\wedge$. The axioms $\bigcirc$-OF-$\bot$ and $\bigcirc$-OF-$\top$ together with BOT and TOP ensure that $\bot$ and $\top$ are flat.

We postulate nothing on $\circledcirc$ because our axiomatization is bound to be incomplete anyway and we will not be needing $\circledcirc$ for the fixed point theorems of Section 4. We *do* state axioms on $\circledcirc$ for the *complete infinitary* axiomatization of sequence algebras in Section 6.2.

3.1.2 Majora and Minora. $\Diamond$-INFLATE and $\Box$-DEFLATE state that $\Diamond$ can only enlarge a sequence whereas $\Box$ can only make it smaller. By $\Diamond$-IDEM and $\Box$-IDEM, $\Diamond$ and $\Box$ are idempotent operations. Intuitively, $\Diamond a$ and $\Box a$ together form the *tightest* monotonic envelope around a. Putting a tightest envelope around the already tightest envelope cannot yield an even tighter one. By $\Diamond$-MONO and $\Box$-MONO, $\Diamond$ and $\Box$ are monotonic. These six axioms together describe that $\Diamond$ and $\Box$ form so-called *closure* or *hull* operators.

Next, by $\bigcirc\Diamond$-COMM and $\bigcirc\Box$-COMM, $\bigcirc$ commutes with $\Diamond$ and $\Box$. For a proof of validity for sequence algebras, see Section A.8.

Finally, we postulate the induction rule $\Diamond$-IND for $\Diamond$: If a is descending, i.e. $\bigcirc a \preceq a$, then $\Diamond a \preceq a$. In fact, then even $\Diamond a = a$ (since $a \preceq \Diamond a$ already holds by $\Diamond$-INFLATE), so taking majora of descending chains has no effect. The converse is also true (indicated by the double inference bar): if $\Diamond a \preceq a$, i.e. taking majorum of a has no effect, then a is descending. For a proof of validity, see Section A.8. The coinduction principle $\Box$-COIND is entirely dual.

3.1.3 Function Applications and Orbits. In sequence algebras, functions are applied *element-wise* to sequences, see Table 2. Naturally, $\bigcirc$ and F must then commute, as postulated by $F\bigcirc$-COMM.

All functions in AIC are *monotonic*, postulated by an axiom F-MONO for every function symbol $F \in \mathrm{Funcs}$. It is not hard to prove that F is monotonic (in the standard sense on single lattice-elements) *if and only if* F-MONO is valid for sequence algebras, see Section A.9.2. Hence, F-MONO captures *precisely* standard monotonicity.

Inherited from standard monotonicity, applying F multiple times is also a monotonic operation. Consequently, F^*-MONO postulates that F^* is monotonic. Contrary to our finitary axiomatization, monotonicity of F^* is provable from monotonicity of F in the complete infinitary axiomatization.

FF^*-COMM postulates that it does not matter whether we first apply F once and then arbitrarily many times or first arbitrarily many times and then once more. In other words, F and F^* commute.

Next, we investigate shifts of orbits. Intuitively, we want $F^* a$ to be the F-orbit of a lattice element. If we left-shift such an orbit, we might expect that this results in F being applied once more, i.e. $\bigcirc F^* a = F F^* a$. However, in AIC a is not a single element but a *sequence* and hence F^* has a more intricate semantics, see Table 2. To be valid under this semantics, the identity ITER for shifting orbits is also more involved.

$$\frac{}{\bigcirc F^* a \;=\; F F^* \bigcirc a}\ \text{ITER}$$

$\bigcirc F^* a$:	$F(a_1)$	$F^2(a_2)$	$F^3(a_3)$	$F^4(a_4)$
$F^* a$:	a_0	$F(a_1)$	$F^2(a_2)$	$F^3(a_3)$
a:	a_0	a_1	a_2	a_3
$\bigcirc a$:	a_1	a_2	a_3	a_4
$F^* \bigcirc a$:	a_1	$F(a_2)$	$F^2(a_3)$	$F^3(a_4)$
$F F^* \bigcirc a$:	$F(a_1)$	$F^2(a_2)$	$F^3(a_3)$	$F^4(a_4)$

The listing on the left may provide some intuition on ITER.

Finally, we postulate (co)induction principles F-IND and F-COIND: If applying F once takes us in a certain direction (with respect to $\preceq$), then F's orbit takes us in the same direction.

Bounded Lattice:

$$\frac{}{a \vee b \;=\; b \vee a}\ \vee\text{-COMM} \qquad \frac{}{a \wedge b \;=\; b \wedge a}\ \wedge\text{-COMM} \qquad \frac{}{(a \vee b) \vee c \;=\; a \vee (b \vee c)}\ \vee\text{-ASSOC} \qquad \frac{}{(a \vee b) \vee c \;=\; a \vee (b \vee c)}\ \vee\text{-ASSOC}$$

$$\frac{}{a \vee (a \wedge b) \;=\; a}\ \vee\text{-ABSORB} \qquad \frac{}{a \wedge (a \vee b) \;=\; a}\ \wedge\text{-ABSORB} \qquad \frac{}{\bot \preceq a}\ \text{BOT} \qquad \frac{}{a \preceq \top}\ \text{TOP}$$

Shifts:

$$\frac{a \preceq b}{\bigcirc a \preceq \bigcirc b}\ \bigcirc\text{-MONO} \qquad \frac{}{\bigcirc \bot \preceq \bot}\ \bigcirc\text{-OF-}\bot \qquad \frac{}{\top \preceq \bigcirc \top}\ \bigcirc\text{-OF-}\top \qquad \frac{}{\bigcirc(a \vee b) \;=\; \bigcirc a \vee \bigcirc b}\ \bigcirc\text{-OVER-}\vee \qquad \frac{}{\bigcirc(a \wedge b) \;=\; \bigcirc a \wedge \bigcirc b}\ \bigcirc\text{-OVER-}\wedge$$

Majora and Minora:

$$\frac{}{a \preceq \Diamond a}\ \Diamond\text{-INFLATE} \qquad \frac{}{\Box a \preceq a}\ \Box\text{-DEFLATE} \qquad \frac{}{\Diamond\Diamond a \;=\; \Diamond a}\ \Diamond\text{-IDEM} \qquad \frac{}{\Box\Box a \;=\; \Box a}\ \Box\text{-IDEM} \qquad \frac{\bigcirc a \preceq a}{\Diamond a \preceq a}\ \Diamond\text{-IND} \qquad \frac{a \preceq \bigcirc a}{a \preceq \Box a}\ \Box\text{-COIND}$$

$$\frac{a \preceq b}{\Diamond a \preceq \Diamond b}\ \Diamond\text{-MONO} \qquad \frac{a \preceq b}{\Box a \preceq \Box b}\ \Box\text{-MONO} \qquad \frac{}{\bigcirc\Diamond a \;=\; \Diamond\bigcirc a}\ \bigcirc\Diamond\text{-COMM} \qquad \frac{}{\bigcirc\Box a \;=\; \Box\bigcirc a}\ \bigcirc\Box\text{-COMM}$$

Function Applications and Orbits:

$$\frac{}{F \bigcirc a \;=\; \bigcirc F a}\ F\bigcirc\text{-COMM} \qquad \frac{a \preceq b}{F a \preceq F b}\ F\text{-MONO} \qquad \frac{a \preceq b}{F^* a \preceq F^* b}\ F^*\text{-MONO} \qquad \frac{}{F F^* a \;=\; F^* F a}\ FF^*\text{-COMM}$$

$$\frac{}{\bigcirc F^* a \;=\; F F^* \bigcirc a}\ \text{ITER} \qquad \frac{F a \preceq a}{F^* a \preceq a}\ F\text{-IND} \qquad \frac{a \preceq F a}{a \preceq F^* a}\ F\text{-COIND}$$

Figure 2: The basic axiom system AIC_0. Above, a, b, c are fixed variables, and F ranges over all function symbols.

3.1.4 Soundness. We have the following theorem whose proof (Section A.8) has been formalized in Isabelle/HOL:

Theorem 10. AIC_0 *is sound for sequence algebras.*

3.2 The Usable Axiom System AIC_1

The extended axiom system AIC_1 is given by AIC_0 plus all axioms shown in Figure 3. Let us go over some of these additional axioms.

3.2.1 Additional Partial Order and Lattice Axioms. AIC_0 axiomatizes algebraically the underlying bounded lattice. AIC_1, through REFLEX, TRANS, and ANTISYMM axiomatizes directly the induced partial order $\preceq$ on the lattice. We will sometimes write

$$\frac{a_1 \preceq a_2 \qquad a_2 \preceq a_3 \qquad \dots \qquad a_{k-1} \preceq a_k}{a_1 \preceq a_k}\ \text{TRANS}^*$$

instead of

$$\dfrac{a_1 \preceq a_2 \qquad \dfrac{a_2 \preceq a_3 \qquad \dfrac{\vdots \qquad \dfrac{a_{k-1} \preceq a_k}{\vdots}\ \text{TRANS}}{a_3 \preceq a_k}\ \text{TRANS}}{a_2 \preceq a_k}\ \text{TRANS}}{a_1 \preceq a_k}\ \text{TRANS}$$

as a shorthand for several intermediate applications of TRANS.

The INDISCERN axiom is morally the congruence rule of equational logic, but for inequalities and for arbitrary terms (not just flat ones of the form $\circledast(a, b, \dots)$). Intuitively, if $u = w$, then we can freely replace term u with term w in any inequality. Formulating this as a rule is slightly more involved: Let $s \preceq t$ be the context in which the subterm u potentially occurs. All to-be-replaced occurrences of u are represented by a placeholder variable a occurring instead of u in s and t and hence $s\,[a\backslash u] \preceq t\,[a\backslash u]$ is the inequality in which occurrences of u are to be replaced with w. If now $u = w$, we can actually make the replacement and conclude that if $s\,[a\backslash u] \preceq t\,[a\backslash u]$ holds, then also $s\,[a\backslash w] \preceq t\,[a\backslash w]$ holds.

$$\frac{s\,[a\backslash u] \;\preceq\; t\,[a\backslash u] \qquad u \;=\; w}{s\,[a\backslash w] \;\preceq\; t\,[a\backslash w]}\ \text{INDISCERN}$$

$$\frac{a \vee b \;\preceq\; b \wedge a \qquad a \;=\; F a}{a \vee b \;\preceq\; b \wedge \boxed{F a}}\ \text{INDISCERN}$$

As an example, the derivation on the left is valid. Here, term s is $a \vee b$, term t is $b \wedge c$, and the placeholder is c. The substitution instance $b \wedge F\,a$ is obtained by replacing every c in $b \wedge c$ by $F\,a$ and $b \wedge a$ is obtained by replacing c with a. Notice that when reading the inference rule from top to bottom, *not every occurrence* of a was replaced by $F\,a$. This is because s was $a \vee b$ but placeholder c does not occur in $a \vee b$.

Just for readability (but with *no* technical necessity), we write $b \wedge \boxed{F\,a}$ (i.e. with a blue marking) below the inference bar to indicate where $F\,a$ replaced a. Intuitively, INDISCERN gives us the flexibility to select only *certain* occurrences of u for replacement by w and we indicate which ones we select in blue.

We will often use INDISCERN implicitly (but rigorously) in the context of identity axioms: Whenever we introduce an identity ABC, we will implicitly introduce an inference rule which is derivable using ABC as the right-hand premise of INDISCERN, *and* we will call this new inference rule also ABC. For example, the identity $\vee$-COMM induces the rule $\vee$-COMM shown in the box above. Its derivation is presented on the right. ASM. indicates an assumption (i.e. a premise above the bar) of an inference rule / quasiequation that we want to derive.

$$\frac{c\,[x\backslash b \vee a] \;\preceq\; d\,[x\backslash b \vee a]}{c\,[x\backslash a \vee b] \;\preceq\; d\,[x\backslash a \vee b]}\ \vee\text{-COMM}$$

$$\frac{\dfrac{}{c\,[x\backslash b \vee a] \;\preceq\; d\,[x\backslash b \vee a]}\ \text{ASM.} \qquad \dfrac{}{a \vee b \;=\; b \vee a}\ \vee\text{-COMM}}{c\,[x\backslash a \vee b] \;\preceq\; d\,[x\backslash a \vee b]}\ \text{INDISCERN}$$

An example of applying the implicit $\vee$-COMM rule on the left-hand-side (were we again indicate in blue the part to which the explicit $\vee$-COMM identity was applied) is shown above right.

$$\frac{b \vee a \;\preceq\; b \wedge a}{a \vee b \;\preceq\; b \wedge a}\ \vee\text{-COMM}$$

Addit. Partial Order and Lattice Axioms:

$$\frac{}{a \preceq a}\ \textsc{reflex} \qquad \frac{a \preceq b \quad b \preceq c}{a \preceq c}\ \textsc{trans} \qquad \frac{s[a\backslash u] \preceq t[a\backslash u] \quad u = w}{s[a\backslash w] \preceq t[a\backslash w]}\ \textsc{indiscern}$$

$$\frac{a \preceq b \quad b \preceq a}{a = b}\ \textsc{antisymm} \qquad \frac{a = b}{a \preceq b}\ \textsc{weakenR} \qquad \frac{a = b}{b \preceq a}\ \textsc{weakenL} \qquad \frac{a \vee b \preceq c}{b \preceq c}\ \vee\textsc{-elim} \qquad \frac{a \preceq b \wedge c}{a \preceq b}\ \wedge\textsc{-elim}$$

$$\frac{}{a \vee a = a}\ \vee\textsc{-idem} \qquad \frac{}{a \wedge a = a}\ \wedge\textsc{-idem} \qquad \frac{a \preceq c \quad b \preceq c}{a \vee b \preceq c}\ \vee\textsc{-introL} \qquad \frac{a \preceq b \quad a \preceq c}{a \preceq b \wedge c}\ \wedge\textsc{-introR} \qquad \frac{b \preceq c}{a \wedge b \preceq c}\ \wedge\textsc{-introL} \qquad \frac{a \preceq b}{a \preceq b \vee c}\ \vee\textsc{-introR}$$

Addit. Majora and Minora Axioms:

$$\frac{a \preceq b}{a \preceq \Diamond b}\ \Diamond\textsc{-introR} \qquad \frac{a \preceq b}{\Box a \preceq b}\ \Box\textsc{-introL} \qquad \frac{\Diamond a \preceq b}{a \preceq b}\ \Diamond\textsc{-elim} \qquad \frac{a \preceq \Box b}{a \preceq b}\ \Box\textsc{-elim}$$

$$\frac{a \preceq b \quad \bigcirc b \preceq b}{\Diamond a \preceq b}\ \Diamond\textsc{-introL} \qquad \frac{a \preceq \bigcirc a \quad a \preceq b}{a \preceq \Box b}\ \Box\textsc{-introR} \qquad \frac{}{\Diamond a = a \vee \bigcirc \Diamond a}\ \Diamond\textsc{-exp} \qquad \frac{}{\Box a = a \wedge \bigcirc \Box a}\ \Box\textsc{-exp} \qquad \frac{}{\bigcirc \Diamond a \preceq \Diamond a}\ \Diamond\textsc{-desc} \qquad \frac{}{\Box a \preceq \bigcirc \Box a}\ \Box\textsc{-asc}$$

Addit. Func. Applic. and Orbit Axioms:

$$\frac{}{\Diamond F a \preceq F \Diamond a}\ \textsc{semi-cont} \qquad \frac{}{F \Box a \preceq \Box F a}\ \textsc{semi-cocont} \qquad \frac{a \preceq \bigcirc a}{F F^* a \preceq \bigcirc F^* a}\ \textsc{asc-iter} \qquad \frac{\bigcirc a \preceq a}{\bigcirc F^* a \preceq F F^* a}\ \textsc{desc-iter}$$

$$\frac{a \preceq F a \quad a \preceq \bigcirc a}{F^* a \preceq \bigcirc F^* a}\ \textsc{orbit-asc} \qquad \frac{\bigcirc a \preceq a \quad F a \preceq a}{\bigcirc F^* a \preceq F^* a}\ \textsc{orbit-desc} \qquad \frac{a \preceq b \quad F b \preceq b}{F^* a \preceq b}\ F^*\textsc{-introL} \qquad \frac{a \preceq F a \quad a \preceq b}{a \preceq F^* b}\ F^*\textsc{-introR}$$

Figure 3: Additional axioms for the automation-friendly axiom system $\mathbf{AIC}_1$. The axiom system $\mathbf{AIC}_1$ contains $\mathbf{AIC}_0$ plus the additional axioms listed above. All additional axioms are *finitely* derivable from $\mathbf{AIC}_0$.

3.2.2 Additional Majora and Minora Axioms. By $\Diamond$-DESC and $\Box$-ASC, majora form descending chains and minora form ascending chains. In fact, we had mentioned earlier that the majorum $\Diamond a$ is the *least decreasing majorant* of a. So if some sequence b is descending ($\bigcirc b \preceq b$) and b is a majorant of a ($a \preceq b$), then b is also a majorant of $\Diamond a$. Dually the minorum $\Box a$ is a's *greatest increasing minorant*. The axioms $\Diamond$-INTROL and $\Box$-INTROR capture precisely this (see Section A.3.3 for a derivation). Finally, much like in LTL, both $\Diamond$ and $\Box$ satisfy an *expansion law* (see Section A.3.2).

3.2.3 Additional Function Application and Orbit Axioms. Any monotonic function is *semi-continuous*. In AIC, this reads $\Diamond F a \preceq F \Diamond a$, stated by SEMI-CONT. Dually, SEMI-COCONT states $F \Box a \preceq \Box F a$. To get a first feel for how to conduct actual AIC-style algebraic proofs, we show the derivation of SEMI-CONT from other axioms:

$$\dfrac{F\text{-MONO}\dfrac{\Diamond\text{-INFLATE}\dfrac{}{a \preceq \Diamond a}}{F a \preceq F \Diamond a} \qquad F\text{-MONO}\dfrac{\Diamond\text{-DESC}\dfrac{}{\bigcirc \Diamond a \preceq \Diamond a}}{F \bigcirc \Diamond a \preceq F \Diamond a}}{\bigcirc F \Diamond a \preceq F \Diamond a}\ F\bigcirc\text{-COMM}}{\Diamond F a \preceq F \Diamond a}\ \Diamond\textsc{-introL}$$

As for additional orbit axioms, we can recover the "naive" version of ITER, namely $\bigcirc F^* a = F F^* a$, for flat sequences: For chains a, the two rules ASC-ITER and DESC-ITER are derivable (see Section A.6). If a is now flat ($a \preceq \bigcirc a \preceq a$), we obtain $\bigcirc F^* a = F F^* a$.

$$\frac{a \preceq \bigcirc a}{F F^* a \preceq \bigcirc F^* a}\ \textsc{asc-iter} \qquad \frac{\bigcirc a \preceq a}{\bigcirc F^* a \preceq F F^* a}\ \textsc{desc-iter}$$

The axioms ORBIT-ASC and ORBIT-DESC assert that certain orbits form chains. This is of interest since chains always converge in our setting and we often want orbits to constitute fixed point iterations that converge to a fixed point. If $a \preceq F a$ and a is ascending, for instance, then the orbit $F^* a$ is provably also ascending. Dually, if $F a \preceq a$ and a is descending, $F^* a$ is also descending.

Finally, we can derive from F-IND and F-COIND rules that are similar to $\Diamond$-INTROL and $\Box$-INTROR, namely F^*-INTROR and F^*-INTROL (see Section A.6.1 for a derivation).

3.3 Continuous Functions

From monotonicity, all functions are necessarily semi-continuous: $\Diamond F a \preceq F \Diamond a$. If the other direction $F \Diamond a \preceq \Diamond F a$ (and thus the identity $F \Diamond a = \Diamond F a$) holds, the function is "fully" continuous. We can state that certain functions F are continuous by additionally postulating *non-derivable* continuity axioms for those functions.

$$\frac{}{F \Diamond a \preceq \Diamond F a}\ \textsc{c-cont} \qquad \frac{}{\Box F a \preceq F \Box a}\ \textsc{c-cocont}$$

More specifically, if we can pull out majora from F without discharging any further premises, this essentially means that one can pull the supremum of any *unordered non-empty countable set* S out from F, i.e. $F(\sup S) = \sup F(S)$. We would then postulate for such functions C-CONT shown above right.

A more commonly used notion of continuity, called ω-*continuity* [1], is when one need not be able to pull out suprema of any unordered set but only of ascending chains. In AIC, this corresponds to being able to pull out majora of ascending chains and we would capture ω-continuity of F by postulating ω-CONT. As with monotonicity, one can prove that F is c- or ω-continuous if and only if the appropriate quasi-inequalities are valid for sequence algebras, see Sections A.9.4 to A.9.6. Notions and axioms for minora and cocontinuity are entirely dual.

$$\frac{a \preceq \bigcirc a}{F \Diamond a \preceq \Diamond F a}\ \omega\textsc{-cont} \qquad \frac{\bigcirc a \preceq a}{\Box F a \preceq F \Box a}\ \omega\textsc{-cocont}$$

4 Algebraic Proofs of Fixed Point Theorems

To demonstrate the usefulness of AIC, we will now present purely algebraic proofs of well- and less-well-known fixed point theorems.

4.1 Kleene, Tarski-Kantorovich, and Park

We first prove in AIC the well-known *Kleene fixed point theorem*[5] [22], or rather a slightly more general result – the *Tarski-Kantorovich principle* (TKP) [16]. It says: for ω-continuous F, if $\ell \sqsubseteq F(\ell)$ then iterating F on ℓ will converge to the least fixed point of F just above ℓ, which we denote by $\mathrm{lfp}_{\sqsupseteq \ell}\, F$:

Theorem 11 (Tarski-Kantorovich Principle). *Let $F\colon L \to L$ be an ω-continuous endomap on a complete lattice L, and $\ell \in L$. Then*

$$\ell \sqsubseteq F(\ell) \quad \text{implies} \quad \mathrm{lfp}_{\sqsupseteq \ell}\, F = \sup_{n\in\omega} F^n(\ell). \qquad \text{(TKP)}$$

Remark 2. TKP and all other fixed point theorems in this section have duals, which emerge by reversing the order (e.g. replace ω-continuous with ω-cocontinous maps and least with greatest fixed points), which can be proved in AIC in the same way. ◁

AIC formalization of Theorem 11. Before we *derive* the theorem, we will first describe how to *formalize* it in AIC. Let us assume some a such that $a \preceq F\,a$ and that ω-cont holds for F. While a is by default any sequence in AIC, a morally takes the role of the single lattice element ℓ. It would thus make sense to require that a is flat, so as to emulate a single lattice element. However, it turns out that this is not necessary, as long as a is ascending, i.e. $a \preceq \bigcirc a$. Note that this makes the theorem we will prove more general. To obtain the classical single-element version of Theorem 11 (TKP), we would instantiate a with the flat sequence $\overline{\ell} = \ell\,\ell\,\ell\,\ell\ldots$ and that sequence is trivially ascending, hence $\overline{\ell} \preceq \bigcirc \overline{\ell}$.

$$\frac{\lfloor F\ \omega\text{-cont} \rfloor \quad a \preceq \bigcirc a \qquad a \preceq F\,a}{F \Diamond F^* a \;=\; \Diamond F^* a}\ \text{TKP-FP}$$

Assuming $a \preceq F\,a$ and $a \preceq \bigcirc a$, we formalize that $\Diamond F^* a$ (cf. $\sup_{n\in\omega} F^n(\ell)$) is the least fixed point of F above a. This comprises proving that (i) $\Diamond F^* a$ is a fixed point, i.e. that TKP-FP shown above right is derivable. By $\lfloor \ldots \rfloor$, we *annotate* which continuity axioms we need to postulate on F (cf. Section 3.3) to prove the rule derivable. This is just for convenience and bears no further formal meaning.

We further formalize that $\Diamond F^* a$ is the *least* fixed point *above* a, i.e. (ii) $\Diamond F^* a$ is itself above a and (iii) any fixed point (and in particular any *pre*fixed point) b above a is also above $\Diamond F^* a$. We thus derive the two quasi-inequalities TKP-ABOVE and TKP-LEAST above.

$$\frac{a \preceq F\,a}{a \preceq \Diamond F^* a}\ \text{TKP-ABOVE} \qquad \frac{a \preceq b \qquad F\,b \preceq b \qquad \bigcirc b \preceq b}{\Diamond F^* a \preceq b}\ \text{TKP-LEAST}$$

Algebraic proof of Theorem 11. For proving TKP-FP, it is useful to first prove that $F^* a$ is a *majoral quasi fixed point*, i.e. *under the scope of a majorum*, it makes no difference whether or not F is applied once more to $F^* a$; formally, $\Diamond F F^* a \;=\; \Diamond F^* a$, which intuitively means that $\Diamond F^* a$ is a fixed point of F *up to continuity*. We divide this identity into the two quasi-inequalities shown in the box above right, and will later reuse these lemmas to prove the Olszewski fixed point theorem.

$$\frac{a \preceq \bigcirc a}{\Diamond F F^* a \preceq \Diamond F^* a}\ \Diamond\text{-QUASI-PRE-FP} \qquad \frac{a \preceq F\,a}{\Diamond F^* a \preceq \Diamond F F^* a}\ \Diamond\text{-QUASI-POST-FP}$$

For a proof of $\Diamond$-QUASI-PRE-FP, consider the upper proof tree on the left; for $\Diamond$-QUASI-POST-FP the lower.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a \preceq \bigcirc a}\,\text{ASM.}}{F F^* a \preceq \bigcirc F^* a}\,\text{ASC-ITER}}{\Diamond F F^* a \preceq \Diamond \bigcirc F^* a}\,\Diamond\text{-MONO}}{\Diamond F F^* a \preceq \bigcirc \Diamond F^* a}\,\bigcirc\Diamond\text{-COMM}}{\Diamond F F^* a \preceq \bigcirc \Diamond F^* a \vee F^* a}\,\vee\text{-INTRO}R}{\Diamond F F^* a \preceq F^* a \vee \bigcirc \Diamond F^* a}\,\vee\text{-COMM}}{\Diamond F F^* a \preceq \Diamond F^* a}\,\Diamond\text{-EXP}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{a \preceq F\,a}\,\text{ASM.}}{F^* a \preceq F^* F\,a}\,F^*\text{-MONO}}{F^* a \preceq F F^* a}\,FF^*\text{-COMM}}{\Diamond F^* a \preceq \Diamond F F^* a}\,\Diamond\text{-MONO}$$

Before we show that $\Diamond F^* a$ is a *proper* fixed point, we would like to point out the seemingly mundane essence of the two proofs shown on the left: *Both are about making one missing F appear.* For $\Diamond$-QUASI-PRE-FP (upper tree), F is missing on the right-hand side and can be created by expanding $\Diamond$, crucially: forgetting the irrelevant $F^* a$, creating a $\bigcirc$ on the non-forgotten part, and this $\bigcirc$ acts on F^* to create the missing F (via iter hidden in asc-iter).

For $\Diamond$-QUASI-POST-FP (the lower tree), F is missing on the left and while we *can* expand the left $\Diamond$, we cannot forget joinees ($\vee$) on the left. Therefore, we instead need that adding F on the right makes that side bigger which is essentially ensured by $a \preceq F\,a$. As a precursor to the Olszewski theorem about $\Box \Diamond F^* a$ we will see later: $a \preceq F\,a$ would not have been necessary if we had some additional $\Box$ guarding $F^* a$. Then we can expand $\Box$ on the left forget the unshifted part of that $\Box$-expansion.

We now show that $\Diamond F^* a$ is a *proper* fixed point: For $\Diamond F^* a$ being a *post*fixed point (TKP-POST-FP), we require only semi-continuity (which all monotonic functions satisfy):

$$\dfrac{\dfrac{}{a \preceq F\,a}\,\text{ASM.}}{\Diamond F^* a \preceq \Diamond F F^* a}\,\Diamond\text{-QUASI-POST-FP} \qquad \dfrac{}{\Diamond F F^* a \preceq F \Diamond F^* a}\,\text{SEMI-CONT}$$
$$\Diamond F^* a \preceq F \Diamond F^* a\ \text{TRANS}$$

For $\Diamond F^* a$ being a *pre*fixed point, we require ω-continuity:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{a \preceq F\,a}\,\text{ASM.}}{F^* a \preceq \bigcirc F^* a}\,\text{ORBIT-ASC}}{F \Diamond F^* a \preceq \Diamond F F^* a}\,\omega\text{-CONT} \qquad \dfrac{\dfrac{}{a \preceq \bigcirc a}\,\text{ASM.}}{\Diamond F F^* a \preceq \Diamond F^* a}\,\Diamond\text{-QUASI-PRE-FP}}{F \Diamond F^* a \preceq \Diamond F^* a}\,\text{TRANS}$$

For c-continuous F, the left branch of the above tree simplifies to:

$$\frac{}{F \Diamond F^* a \preceq \Diamond F F^* a}\,\text{C-CONT}$$

Remark 12 (Prefixed Points of c-continuous Maps). As a by-product, we have shown for ascending a that $\Diamond F^* a$ is a prefixed point of any c-continuous map F. Indeed, $a \preceq F\,a$ is *not* required for being a prefixed point. In the classical single-lattice-element setting this reads: If F is c-continuous, then $\sup_{n\in\omega} F^n(\ell)$ is a prefixed point of F for any $\ell \in L$. While a minor result, this is to the best of our knowledge a novel result. ◁

[5] Though for our restricted setting where the lattice is countably complete.

We can combine the just proven $\Diamond F^* a \preceq F \Diamond F^* a$ and $F \Diamond F^* a \preceq \Diamond F^* a$ using ANTISYMM to obtain the desired quasiequation TKP-FP. It is then left to prove TKP-ABOVE and TKP-LEAST. For TKP-ABOVE, see the proof tree above right. For TKP-LEAST, we have the proof tree below, thus completing the algebraic proof of Theorem 11.

$$\dfrac{\dfrac{\dfrac{}{a \preceq Fa}\,\text{ASM.}}{a \preceq F^* a}\,F\text{-IND}}{a \preceq \Diamond F^* a}\,\Diamond\text{-INTRO}$$

$$\dfrac{\dfrac{\dfrac{}{a \preceq b}\,\text{ASM.} \quad \dfrac{}{Fb \preceq b}\,\text{ASM.}}{F^* a \preceq b}\,F^*\text{-INTROL} \qquad \dfrac{}{\bigcirc b \preceq b}\,\text{ASM.}}{\Diamond F^* a \preceq b}\,\Diamond\text{-INTROL}$$

□

We obtain the Kleene fixed point theorem as an immediate corollary of the Tarski-Kantorovich principle, namely by instantiating $a = \bot$ to obtain the very least fixed point (i.e. the least one above $\bot$), then given by $\Diamond F^* \bot$ (cf. $\sup_n F^n(\bot)$).

We can also read this corollary off the AIC proof of TKP. This is because wherever $a \preceq \bigcirc a$ or $a \preceq F a$ occur as assumptions in our proofs and we have $a = \bot$, we can vacuously discharge these assumptions by applying the axiom BOT. Similarly, the Park induction principle [28] for upper-bounding least fixed points of continuous functions F, i.e.

$$\forall \ell \in L\colon \qquad F(\ell) \sqsubseteq \ell \quad \text{implies} \quad \mathsf{lfp}\, F \sqsubseteq \ell$$

is an immediate instance of TKP-FP, TKP-ABOVE, TKP-LEAST for $a = \bot$ and $b = \ell\ \ell\ \ell\ \ell \ldots$. In fact, we can readily read off our algebraic proofs a *generalized* Park induction principle:

THEOREM 13 (GENERALIZED PARK INDUCTION). *Let $\ell, m \in L$ and $F\colon L \to L$ be ω-continuous. Then*

$$m \sqsubseteq F(m) \ \wedge\ m \sqsubseteq \ell \ \wedge\ F(\ell) \sqsubseteq \ell \quad \Longrightarrow \quad \mathsf{lfp}_{\sqsupseteq m}\, F \sqsubseteq \ell\,.$$

PROOF. Instantiate TKP-FP and TKP-ABOVE with $a = m\ m\ m\ m \ldots$ and $b = \ell\ \ell\ \ell\ \ell \ldots$ (both flat). It follows that $[\![\Diamond F^* a]\!]_0 = \mathsf{lfp}_{\sqsupseteq m}\, F$, and thus $\mathsf{lfp}_{\sqsupseteq m}\, F \sqsubseteq \ell$ by TKP-LEAST. □

4.2 Olszewski

By the Tarski-Kantorovich principle (Theorem 11), seeding the iteration of an ω-(co)continuous map F with a pre- or postfixed point of F converges to a *proper* fixed point. But how to find pre- or postfixed points to begin with? A recent result due to Olszewski shows that they emerge by iterating on an *arbitrary* seed element.

THEOREM 14 (OLSZEWSKI [27]). *Let $F\colon L \to L$ be ω-cocontinuous and $\ell \in L$. Then $\inf_{n\in\omega} \sup_{k\geq n} F^k(\ell)$ is a postfixed point of F.*

We recall Olszewski's argument in Section A.10 for the convenience of the reader. Under stronger assumptions on F, we can improve on Olszewski's result and obtain *proper* fixed points:

THEOREM 15. *Let $F\colon L \to L$ be ω-cocontinuous and c-continuous and $\ell \in L$. Then $\inf_{n\in\omega} \sup_{k\geq n} F^k(\ell)$ is a fixed point of F.*

Remark 3. There is also a transfinite version of Theorem 14 that only assumes monotonicity of F, see [26, Thm. 1]. Similarly to the transfinite version of the Knaster-Tarski Theorem by Cousot and Cousot [10], this result is currently out of scope of AIC. ◁

$$\dfrac{\lceil F\ \omega\text{-COCONT} \rfloor \quad \bigcirc a \preceq a}{\Box\Diamond F^* a \preceq F \Box\Diamond F^* a}\,\text{OL-POST-FP}$$

$$\dfrac{\lceil F\ \text{C-CONT} \rfloor \quad a \preceq \bigcirc a}{F \Box\Diamond F^* a \preceq \Box\Diamond F^* a}\,\text{OL-PRE-FP}$$

$$\dfrac{\lceil F\ \omega\text{-COCONT}, F\ \text{C-CONT} \rfloor \quad \bigcirc a \preceq a \qquad a \preceq \bigcirc a}{\Box\Diamond F^* a = F \Box\Diamond F^* a}\,\text{OL-FP}$$

AIC FORMALIZATION OF THEOREM 14 AND THEOREM 15. As in Section 4.1, the fixed seed element ℓ is associated with a variable a. Theorem 14 then reads in AIC as OL-POST-FP shown above left, where – analogously to the AIC formalization of Theorem 11 – we prove a more general statement and hence have an additional premise $\bigcirc a \preceq a$. Theorem 14 is obtained from instantiating a with the flat sequence $\ell\ \ell\ \ell\ \ell \ldots$, for which this premise holds vacuously. Similarly, Theorem 15 is formalized as OL-FP shown above.

$$\dfrac{\bigcirc a \preceq a}{\Box\Diamond F^* a \preceq \Box\Diamond F F^* a}\,\Box\Diamond\text{-QUASI-POST-FP}$$

$$\dfrac{a \preceq \bigcirc a}{\Box\Diamond F F^* a \preceq \Box\Diamond F^* a}\,\Box\Diamond\text{-QUASI-PRE-FP}$$

ALGEBR. PROOF OF THEOREM 14 AND THEOREM 15. Similarly to the proof of TKP-FP, it is useful to first prove that $F^* a$ is a *mino-majoral quasi fixed point of F*, i.e. *under the scope of a nested minorum-majorum*, it makes no difference whether or not F is applied once more to $F^* a$; formally, $\Box\Diamond F F^* a = \Box\Diamond F^* a$. Thus, we derive the two rules $\Box\Diamond$-QUASI-POST-FP and $\Box\Diamond$-QUASI-PRE-FP shown in the box above.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\bigcirc a \preceq a}{\bigcirc F^* a \preceq F F^* a}\,\text{DESC-ITER}}{\Diamond \bigcirc F^* a \preceq \Diamond F F^* a}\,\Diamond\text{-MONO}}{\bigcirc\Diamond F^* a \preceq \Diamond F F^* a}\,\bigcirc\Diamond\text{-COMM}}{\Box \bigcirc \Diamond F^* a \preceq \Box \Diamond F F^* a}\,\Box\text{-MONO}}{\bigcirc\Box\Diamond F^* a \preceq \Box\Diamond F F^* a}\,\bigcirc\Box\text{-COMM}}{\Diamond F^* a \wedge \bigcirc\Box\Diamond F^* a \preceq \Box\Diamond F F^* a}\,\wedge\text{-INTROL}}{\Box\Diamond F^* a \preceq \Box\Diamond F F^* a}\,\Box\text{-EXP}$$

For $\Box\Diamond$-QUASI-POST-FP, consider the upper left proof tree. Here, we can expand a $\Box$ on the left, which we did not have available for proving $\Diamond$-QUASI-POST-FP. This is the algebraic essence of why Olszewski will not require $a \preceq F a$ or alike.

$$\dfrac{\dfrac{a \preceq \bigcirc a}{\Diamond F F^* a \preceq \Diamond F^* a}\,\Diamond\text{-QUASI-PRE-FP}}{\Box\Diamond F F^* a \preceq \Box\Diamond F^* a}\,\Box\text{-MONO}$$

For $\Box\Diamond$-QUASI-PRE-FP, we have the lower proof tree. Notice that we re-used the $\Diamond$-QUASI-PRE-FP rule from the proof of TKP. Using $\Box\Diamond$-QUASI-POST-FP, we prove OL-POST-FP in Figure 4 (top). Finally, with OL-POST-FP at hand, the derivation of OL-FP follows immediately from OL-PRE-FP which we derive also in Figure 4 (bottom), thus concluding our algebraic proofs of Theorem 14 and Theorem 15. □

4.3 Latticed k-Induction

Latticed k-induction [6] is a fixed point-theoretic generalization of the prominent k-induction verification principle [31] for hard- and software model checking [7, 11, 14, 17]. It has successfully been employed for the verification of probabilistic programs [6, 36] and probabilistic pushdown systems [35].

Fix an ω-continuous $F\colon L \to L$ and an element $\ell \in L$. We call $G_\ell\colon L \to L$ defined as $G_\ell(m) = F(m) \sqcap \ell$ the *k-Induction operator*. The principle of k-induction is a generalization of Park induction:

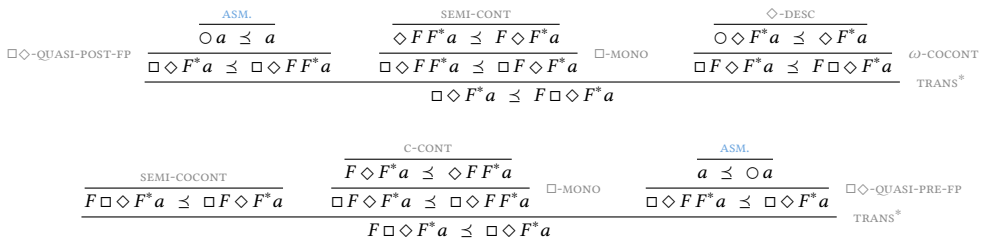


Figure 4: Proof of OL-POST-FP (top tree) and OL-PRE-FP (bottom tree).

THEOREM 16 (LATTICED k-INDUCTION [6]). *For every $k \in \mathbb{N}$,*

$$F\big(G_\ell^k(\ell)\big) \sqsubseteq \ell \qquad \text{implies} \qquad \mathsf{lfp}\, F \sqsubseteq \ell\,.$$

AIC FORMALIZATION OF THEOREM 16. Analogously to Section 4.1, we associate the fixed lattice element ℓ with a fixed b. To formalize the k-fold application of the k-induction operator, we define for all $k \in \mathbb{N}$ the term $G_b^k\, b$ recursively by

$$G_b^k\, b \;=\; \begin{cases} b & \text{if } k = 0 \\ F\, G_b^{k-1}\, b \;\wedge\; b & \text{otherwise}\,. \end{cases}$$

The above is meant to define *syntactic* equality of terms, so e.g. defining that $G_b^2\, b$ is a name for the term $F\, G_b^1\, b \wedge b$.

The algebraic version of Theorem 16 then reads as a family of quasi-inequalities k-IND (shown right, parametrized in k). We require the additional premise $\bigcirc b \preceq b$ for the same reasons as in the formalization of Theorem 11. Classical k-induction (Theorem 16) is obtained from k-IND for $b = \ell\,\ell\,\ell\,\ell\ldots$ for which $\bigcirc b \preceq b$ holds vacuously. We prove k-IND enitrely within AIC_1 for every $k \in \mathbb{N}$ (cf. Section A.11.4), constructing proofs inductively on k.

$$\frac{\overset{\wr F\ \omega\text{-CONT}\int}{F\, G_b^k\, b \preceq b} \qquad \bigcirc b \preceq b}{\Diamond F^* \bot \preceq b}\ k\text{-IND}$$

5 Mechanization

We mechanized AIC in Isabelle/HOL to confirm soundness and usability. The mechanization is a shallow embedding of sequence algebras on complete lattices as presented in Section 2. A shallow embedding means we do not separately formalize the algebra as an object or define its syntax. Instead, we directly build on Isabelle/HOL's formalization of complete lattices and define the operators of the algebra as functions and constants in Isabelle. We use functions from natural numbers to lattice elements as the type of sequences. With this, the definition of operators is straightforward, and integrates so well into the existing Isabelle lattice setup that for instance our $\wedge$ and $\vee$ coincide with existing Isabelle type class operators $\sqcup$ and $\sqcap$ applied to functions.

The equations and reasoning rules of the algebra can then be derived as lemmas in Isabelle from the definition of the operators. This builds up the algebra in the prover and at the same time constitutes a soundness proof of AIC_0 as well as any derived rules.

Using our formalization, we proved all fixed point theorems of Section 4. The proofs follow the paper presentation, with intermediate steps solved fully automatically by Isabelle's sledgehammer.

Beyond that, if the extended axiom system AIC_1 is available, *sledgehammer is even able to prove many high-level theorems such as Tarski-Kantorovich or Park induction fully automatically.* We also found that Isabelle's counter-example finder is effective in identifying misstated lemmas. Both show promise for the use of the algebra and further exploration of fixed point principles directly in the prover. Conversely, if we remove important derivable rules such as ITER and ◇-EXP as explicit lemma statements and force the prover to work directly with expanded definitions and indexed suprema and infima as in traditional fixed point formalizations, automation tends to break down quickly. Sledgehammer is able to recover some of these by reproving them inline, but higher-level theorems remain out of reach. This means that the abstraction of the algebra brings with it not only increased clarity, but also improves proof search.

6 Completeness and Incompleteness

In this section, we investigate aspects of completeness of the axiom systems presented in Section 3. Completeness of AIC_0 means that if a finitary quasiequation is valid for sequence algebras, then it is derivable from AIC_0. In this section, we show that AIC_0 is *not* complete. In fact, even if we restrict just to the ◎ and ○ operations, no finite axiom system of finitary quasiequations can be complete. This situation changes when allowing *infinitary* quasiequations and a slightly infinite notion of derivation, as we will see in Section 6.2.

6.1 Incompleteness of Finitary Axiomatizations

We now show that the validity of finitary quasiequations that just involve the ◎ and ○ operations has no sound and complete finite axiomatization. To this end, it suffices to consider a simplified version of sequence algebras that drops all lattice-theoretic structure.

Definition 17. A *discrete sequence algebra* is given by the set A^ω of sequences in a set A equipped with the two unary operations $◎, ○ \colon A^\omega \to A^\omega$ defined exactly the same as in Definition 2 (2.3). ◁

All syntactic concepts for sequence algebras (terms, quasiequations, finite derivations) carry over to discrete sequence algebras by restricting all definitions to ◎ and ○. We speak of *discrete* terms, quasiequations, etc. for distinction. For instance, a discrete quasiequation is a quasiequation whose terms use only ◎ and ○.

A discrete quasiequation is *valid for discrete sequence algebras* if it is satisfied by every discrete sequence algebra. A discrete axiom system Ax (i.e. a set of discrete finitary quasiequations) is *sound* for discrete sequence algebras if every quasiequation from Ax is valid for discrete sequence algebras. It is *complete* for discrete sequence

algebras if every quasiequation that is valid for discrete sequence algebras has a finite derivation from Ax.

Theorem 18 (Incompleteness). *There is no finite discrete axiom system that is both sound and complete for discrete sequence algebras.*

Intuitively, the reason is that a finite discrete axiom system cannot derive non-trivial statements about periodic sequences with large periods, since the finitely many finitary axioms necessarily only contain statements about periods of bounded length. Specifically, for each positive integer N, consider the discrete quasiequation

$$\bigcirc^N a = a \quad \wedge \quad \bigwedge_{i=0}^{N-1} \circledcirc \bigcirc^i a = \circledcirc \bigcirc^{i+1} a \quad \Longrightarrow \quad \bigcirc a = a \tag{6.1}$$

stating that if a sequence is periodic with period length N and its first N elements are equal, then the sequence is flat. While (6.1) is valid for discrete sequence algebras, one can show that for every finite and sound discrete axiom system Ax, this quasiequation is not derivable from Ax for sufficiently large N. Thus Ax is not complete.

Despite the simple underlying idea, the proof of Theorem 18 is fairly involved; it rests on the introduction of a suitable normal form for quasiequations and a careful analysis of possible derivations from normalized quasiequations. For details, see Section A.12.

6.2 A Complete Infinitary Axiomatization

As we have just seen, no finite set of finitary quasiequations can completely capture validity. For achieving completeness, we need to add possibly *infinitary* quasiequations, i.e. $(\bigwedge_{i\in I} {}^i s = {}^i t) \Longrightarrow s = t$ where I may be infinite. As the size of I determines the branching degree in derivation trees, we can no longer be satisfied with our finite derivation trees (cf. Definition 7). It turns out that a slightly different kind of finiteness provides just the right notion of derivation for infinitary quasiequational logic.

Definition 19 (Well-founded Derivation). An inference tree is *well-founded* if every branch of the tree has finite height. Given an axiom system Ax and an quasiequation Q, a *well-founded* derivation of Q from Ax is defined exactly as in Definition 7, except that the underlying inference tree is well-founded in lieu of finite. A quasiequation Q is *well-foundedly derivable from* Ax, denoted $\mathsf{Ax} \vdash_{\mathsf{wf}} \mathsf{Q}$, if Q has a well-founded derivation from Ax. ◁

By Kőnig's lemma, a finitely branching well-founded tree is finite. Thus our previous notion of finite derivability (Definition 7) coincides with well-founded derivability when all of the quasiequations from Ax are finitary. In particular, since all AIC_0 axioms are finitary, a quasiequation Q is derivable from AIC_0 if and only if $\mathsf{AIC}_0 \vdash_{\mathsf{wf}} \mathsf{Q}$.

Importantly, we also cannot be satisfied with inference trees of finite height, even with infinitary branching. Indeed, if Ax could contain $(\bigwedge_{i\in I} {}^i s = {}^i t) \Longrightarrow s = t$ with $I = \omega$ and each identity ${}^i s = {}^i t$ with a derivation of height i, like so:

$$\dfrac{\dfrac{}{{}^0 s = {}^0 t}\,\text{(derivation height 0)} \quad \dfrac{\dfrac{\cdots}{{}^1 s = {}^1 t}\,\text{(derivation height 1)} \quad \dfrac{\dfrac{\cdots}{{}^2 s = {}^2 t}\,\text{(derivation height 2)} \quad \cdots}{\cdots}}{\cdots}}{s = t}$$

This is a derivation tree of infinite height, but it also well-founded, because every branch has finite height. To summarize, well-founded derivations are sufficient and (in general) necessary for reasoning with infinitary inference rules. This is the content of the theorem below, which appears to be folklore.[6] We state the theorem for AIC-structures, but it extends to algebras over any finitary signature.

Table 3: Axioms of AIC_ω ($a, b, c \in$ Vars are fixed variables).

Lattice:	$\bot \preceq a \qquad a \preceq \top \qquad a \vee b = b \vee a \qquad a \wedge b = b \wedge a$ $a \wedge (a \vee b) = a = a \vee (a \wedge b) \qquad a \preceq b \Longrightarrow Fa \preceq Fb$ $a \wedge (b \wedge c) = (a \wedge b) \wedge c \qquad a \vee (b \vee c) = (a \vee b) \vee c$
Head:	$\circledcirc \bot = \bot \qquad \circledcirc \top = \top \qquad \circledcirc (a \wedge b) = \circledcirc a \wedge \circledcirc b \qquad \circledcirc (a \vee b) = \circledcirc a \vee \circledcirc b$ $\circledcirc Fa = F \circledcirc a \qquad \circledcirc F^* a = \bigcirc \circledcirc a = \Diamond \circledcirc a = \Box \circledcirc a = \circledcirc \circledcirc a = \circledcirc a$
Shift:	$\bigcirc \bot = \bot \qquad \bigcirc \top = \top \qquad \bigcirc (a \vee b) = \bigcirc a \vee \bigcirc b \qquad \bigcirc (a \wedge b) = \bigcirc a \wedge \bigcirc b$ $\bigcirc Fa = F \bigcirc a \qquad \bigcirc F^* a = FF^* \bigcirc a \qquad \bigcirc \Diamond a = \Diamond \bigcirc a \qquad \bigcirc \Box a = \Box \bigcirc a$
Majorum/ Minorum:	$a \preceq \Diamond a \qquad \Box a \preceq a \qquad \Diamond \Diamond a = a \qquad \Box \Box a = a$ $\bigcirc a \preceq a \iff \Diamond a \preceq a \qquad a \preceq \bigcirc a \iff a \preceq \Box a$
Sequence:	$\bigwedge_{n\in\omega} \circledcirc \bigcirc^n a \preceq b \Longrightarrow \circledcirc \Diamond a \preceq b \qquad \bigwedge_{n\in\omega} b \preceq \circledcirc \bigcirc^n a \Longrightarrow b \preceq \circledcirc \Box a$ $\bigwedge_{n\in\omega} \circledcirc \bigcirc^n a = \circledcirc \bigcirc^n b \Longrightarrow a = b$

Theorem 20 (Soundness and Completeness of Well-founded Derivations). *Let* Ax *be an axiom system and let* Q *be a quasiequation. Then* $\mathsf{Ax} \vdash_{\mathsf{wf}} \mathsf{Q}$ *if and only if for any AIC-structure* $\mathcal{A} \models \mathsf{Ax}$*, we also have* $\mathcal{A} \models \mathsf{Q}$.

An *infinitary* axiom system AIC_ω that is sound and complete for sequence algebras is given in Table 3. (For economy of space, we present the axioms as implications rather than inference rules.) Note that there are exactly three infinitary axioms, namely the sequence axioms found at the bottom of Table 3.

Theorem 21 (Soundness and Completeness of AIC_ω). *For any quasiequation* Q,

$$\mathsf{AIC}_\omega \vdash_{\mathsf{wf}} \mathsf{Q} \qquad \text{iff} \qquad \mathsf{Q} \text{ is valid for sequence algebras.}$$

The proof of Theorem 21 uses two results: The first one is Theorem 20, which tells us that to show that a quasiequation is well-foundedly derivable in AIC_ω, it suffices to show that it is true in all models (not just sequence algebras) of AIC_ω. The second result is the AIC_ω *embedding theorem* below, which tells us that every AIC-structure that satisfies AIC_ω embeds into some sequence algebra.

Theorem 22 (AIC_ω-Embedding). *Let* $\mathcal{A}_0 \models \mathsf{AIC}_\omega$ *be an AIC-structure. Then there exists a complete lattice* $(L, \sqsubseteq)$ *and a sequence algebra* $\mathcal{A}$ *carried by* L^ω *such that* $\mathcal{A}_0$ embeds *into* $\mathcal{A}$*, in the sense that there exists an injective algebra homomorphism* $\varepsilon \colon \mathcal{A}_0 \hookrightarrow \mathcal{A}$.

Proof Sketch of Theorem 22. Given an AIC-structure $\mathcal{A}_0 \models \mathsf{AIC}_\omega$, we first need to find a complete lattice L, which later will carry the sequence algebra $\mathcal{A}$. We start by defining a (possibly incomplete) lattice L_0 as follows: let A_0 carry $\mathcal{A}_0$, and define $L_0 = \{\circledcirc^{\mathcal{A}_0} x \mid x \in A_0\}$. Note that $L_0 \subseteq A_0$. From the first row of the head axioms in Table 3, we see that L_0 is a lattice when equipped with the lattice operations of $\mathcal{A}_0$: given $x, y \in A_0$, we define

$$\top^{L_0} = \circledcirc^{\mathcal{A}_0} \top^{\mathcal{A}_0} \qquad \text{and} \qquad \circledcirc^{\mathcal{A}_0} x \sqcap^{L_0} \circledcirc^{\mathcal{A}_0} y = \circledcirc^{\mathcal{A}_0} (x \wedge^{\mathcal{A}_0} y)$$

and similarly for $\bot^{L_0}$ and $\sqcup^{L_0}$. Furthermore, for each $F \in$ Funcs, the operation $F^{\mathcal{A}_0}$ restricts to a monotone map $F^{L_0} \colon L_0 \to L_0$ defined

[6] For the sake of convenience, a proof can be found in the appendix.

by $F^{L_0}(\circledcirc^{\mathcal{A}_0} x) = \circledcirc^{\mathcal{A}_0} F^{\mathcal{A}_0}(x)$ for each $x \in A_0$ by the bottom-left equation in the Head Axioms of Table 3.

The only issue with stopping here and declaring that $L = L_0$ is that L_0 may be incomplete. This is where we make use of a theorem of Macneille [23], which states that every lattice L_0 admits an order-embedding into a complete lattice L called the *Dedekind-Macneille completion of* L_0. So, let $m\colon L_0 \hookrightarrow L$ be the Dedekind-Macneille completion of L_0. Every monotone map $F_0\colon L_0 \to L_0$ extends to a (not necessarily unique) monotone map $F\colon L \to L$, in the sense that $F \circ m = m \circ F_0$; see [33, Proposition 3.3].

Thus, we arrive at the sequence algebra $\mathcal{A}$ and the injective algebra homomorphism $\mathcal{A}_0 \hookrightarrow \mathcal{A}$ that we were looking for. The sequence algebra $\mathcal{A}$ is carried by L^ω, where L is the Dedekind-Macneille completion of L_0, and for each function symbol $F \in$ Funcs, the operation $F^{\mathcal{A}}$ is the one obtained from some extension of $F^{L_0}\colon L_0 \to L_0$ to a monotone map $F^L\colon L \to L$ (see Definition 2). The embedding $\varepsilon\colon A_0 \to L^\omega$ is then obtained by forming sequences using the head and shift operators: for any $x \in A_0$ and $n \in \omega$, we set $\varepsilon(x)_n = m(\circledcirc \circ {}^n x)$. Since m is an order-embedding, it follows from the last axiom in the Sequence Axioms row of Table 3 that ε is injective. Verifying that ε is an algebra homomorphism amounts to a long calculation; see appendix for details. □

Proof of Theorem 21. Soundness ($\Rightarrow$) holds by Theorem 20 and the observation that all axioms in AIC_ω are valid for sequence algebras. For completeness ($\Leftarrow$), consider any quasiequation Q and suppose that for any sequence model $\mathcal{A}$, $\mathcal{A} \models \mathrm{Q}$. We need to show that $\mathsf{AIC}_\omega \vdash_{\mathsf{wf}} \mathrm{Q}$. By Theorem 20, it suffices to argue that $\mathcal{A}_0 \models \mathrm{Q}$ for any AIC-structure $\mathcal{A}_0$ that satisfies AIC_ω. But given any such $\mathcal{A}_0$, by Theorem 22 there is an injective algebra homomorphism $\varepsilon\colon \mathcal{A}_0 \hookrightarrow \mathcal{A}$ into some sequence algebra $\mathcal{A}$. Quasiequations are universally quantified, so whenever an algebra satisfies some quasiequation, so do all its subalgebras. Therefore, from our assumption that $\mathcal{A} \models \mathrm{Q}$ it follows that $\mathcal{A}_0 \models \mathrm{Q}$, as desired. □

7 Limitations and Outlook

AIC currently cannot reason about *transfinite* fixed point iterations. If it could, this might enable reasoning about fixed points of *arbitrary monotonic* endomaps, e.g. by algebraizing the constructive version of the Knaster-Tarski theorem by Cousot and Cousot [10].

As for a connection to modal logics, linear time temporal logic (LTL) [29] seems to be very related to the sequence-part of AIC. While the purpose of LTL is completely different and it does not have iteration operations, it would still be interesting to investigate how strong the connection between LTL and AIC really is. The fact that both AIC and LTL admit expansion laws as well as absorption laws a là $\Diamond \Box \Diamond a = \Box \Diamond a$ suggests that the connection is strong.

In verification, one could investigate whether Olszewski-type fixed points admit a temporal interpretation a là "$\Box \Diamond F^* a$ are the states that always eventually reach a by taking F-transitions".

Another promising direction for future work is to study non-standard (i.e. non-sequence) models of AIC. From Theorem 21 applied to the axiom system AIC_0 and the incompleteness result of Section 6.1, it follows that many such models exist. We leave it as future work to discover interesting examples of non-standard models. Particularly interesting would be models where the inhabitants can also have a sort of "orientation" or "polarity" à la ascending/descending. Possible candidates for such structures would be trees, directed sets, continuous real-valued functions, or permutations.

References

[1] Samson Abramsky and Achim Jung. 1994. Domain theory. (1994).

[2] Jirí Adámek, Stefan Milius, and Jirí Velebil. 2007. What Are Iteration Theories?. In *Mathematical Foundations of Computer Science 2007, 32nd International Symposium, MFCS 2007, Ceský Krumlov, Czech Republic, August 26-31, 2007, Proceedings (Lecture Notes in Computer Science, Vol. 4708)*, Ludek Kucera and Antonín Kucera (Eds.). Springer, 240–252. doi:10.1007/978-3-540-74456-6_23

[3] Paolo Baldan, Richard Eggert, Barbara König, and Tommaso Padoan. 2023. Fixpoint Theory - Upside Down. *Log. Methods Comput. Sci.* 19, 2 (2023).

[4] Paolo Baldan, Barbara König, and Tommaso Padoan. 2024. Systems of fixpoint equations: Abstraction, games, up-to techniques and local algorithms. *Inf. Comput.* 301 (2024), 105233.

[5] Kevin Batz, Mingshuai Chen, Benjamin Lucien Kaminski, Joost-Pieter Katoen, Christoph Matheja, and Philipp Schröer. 2021. Latticed k-Induction with an Application to Probabilistic Programs. *CoRR* abs/2105.14100 (2021). arXiv:2105.14100 https://arxiv.org/abs/2105.14100

[6] Kevin Batz, Mingshuai Chen, Benjamin Lucien Kaminski, Joost-Pieter Katoen, Christoph Matheja, and Philipp Schröer. 2021. Latticed k-Induction with an Application to Probabilistic Programs. In *CAV (2) (Lecture Notes in Computer Science, Vol. 12760)*. Springer, 524–549.

[7] Dirk Beyer, Matthias Dangl, and Philipp Wendler. 2015. Boosting k-Induction with Continuously-Refined Invariants. In *CAV (1) (Lecture Notes in Computer Science, Vol. 9206)*. Springer, 622–640.

[8] Stephen L. Bloom and Zoltán Ésik. 1993. *Iteration Theories - The Equational Logic of Iterative Processes.* Springer. doi:10.1007/978-3-642-78034-9

[9] Edmund M. Clarke. 1977. Program Invariants as Fixed Points. In *FOCS*. IEEE Computer Society, 18–29.

[10] Patrick Cousot and Radhia Cousot. 1979. Constructive versions of Tarski's fixed point theorems. *Pacific journal of Mathematics* 82, 1 (1979), 43–57.

[11] Alastair F. Donaldson, Leopold Haller, Daniel Kroening, and Philipp Rümmer. 2011. Software Verification Using k-Induction. In *SAS (Lecture Notes in Computer Science, Vol. 6887)*. Springer, 351–368.

[12] Frank M. V. Feys and Helle Hvid Hansen. 2019. Arrow's Theorem Through a Fixpoint Argument. In *TARK (EPTCS, Vol. 297)*. 175–188.

[13] Carl A Gunter. 1992. *Semantics of programming languages: structures and techniques.* MIT press.

[14] Arie Gurfinkel and Alexander Ivrii. 2017. K-induction without unrolling. In *FMCAD*. IEEE, 148–155.

[15] M. W. Hirsch and Hal Smith. 2005. Monotone maps: a review. *Journal of Difference Equations and Applications* 11, 4-5 (2005), 379–398. doi:10.1080/10236190412331335445

[16] Jacek Jachymski, Leslaw Gajek, and Piotr Pokarowski. 2000. The Tarski–Kantorovitch Prinicple and the Theory of Iterated Function Systems. *Bulletin of the Australian Mathematical Society* 61, 2 (2000), 247–261.

[17] Dejan Jovanovic and Bruno Dutertre. 2016. Property-directed k-induction. In *FMCAD*. IEEE, 85–92.

[18] Tomasz Kiwerski and Jakub Tomaszewski. 2024. Arithmetic, interpolation and factorization of amalgams. arXiv:2401.05526 [math.FA] https://arxiv.org/abs/2401.05526

[19] Barbara König. 2024. Approximating Fixpoints of Approximated Functions (Invited Talk). In *CSL (LIPIcs, Vol. 288)*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 4:1–4:1.

[20] Dexter Kozen. 1982. Results on the Propositional μ-Calculus. In *Automata, Languages and Programming, 9th Colloquium, Aarhus, Denmark, July 12-16, 1982, Proceedings (Lecture Notes in Computer Science, Vol. 140)*, Mogens Nielsen and Erik Meineche Schmidt (Eds.). Springer, 348–359. doi:10.1007/BFB0012782

[21] D. Kozen. 1994. A Completeness Theorem for Kleene Algebras and the Algebra of Regular Events. *Information and Computation* 110, 2 (1994), 366–390. doi:10.1006/inco.1994.1037

[22] Jean-Louis Lassez, V. L. Nguyen, and Liz Sonenberg. 1982. Fixed Point Theorems and Semantics: A Folk Tale. *Inform. Process. Lett.* 14, 3 (1982), 112–116.

[23] H. M. MacNeille. 1936. Partially ordered sets. (1936). doi:10.1090/S0002-9947-1937-1501929-X

[24] Jayadev Misra. 2001. A walk over the shortest path: Dijkstra's Algorithm viewed as fixed-point computation. *Inf. Process. Lett.* 77, 2-4 (2001), 197–200.

[25] John F. Nash. 1950. Equilibrium points in n-person games. *Proceedings of the National Academy of Sciences* 36, 1 (1950), 48–49. doi:10.1073/pnas.36.1.48

[26] Wojciech Olszewski. 2021. On Convergence of Sequences in Complete Lattices. *Order* 38 (2021), 251–255.

[27] Wojciech Olszewski. 2021. On sequences of iterations of increasing and continuous mappings on complete lattices. *Games and Economic Behavior* 126 (2021), 453–459.

[28] David Park. 1969. Fixpoint Induction and Proofs of Program Properties. *Machine Intelligence* 5 (1969).
[29] Amir Pnueli. 1977. The Temporal Logic of Programs. In *18th Annual Symposium on Foundations of Computer Science, Providence, Rhode Island, USA, 31 October - 1 November 1977*. IEEE Computer Society, 46–57. doi:10.1109/SFCS.1977.32
[30] Alejandro Santacruz Hidalgo and Gord Sinnamon. 2024. Core decreasing functions. *Journal of Functional Analysis* 287, 4 (2024), 110490. doi:10.1016/j.jfa.2024.110490
[31] Mary Sheeran, Satnam Singh, and Gunnar Stålmarck. 2000. Checking Safety Properties Using Induction and a SAT-Solver. In *FMCAD (Lecture Notes in Computer Science, Vol. 1954)*. Springer, 108–125.
[32] Gord Sinnamon. 2007. Monotonicity in Banach function spaces. *Nonlinear Analysis, Function Spaces and Applications* (2007), 205–240.
[33] Mark Theunissen and Yde Venema. 2007. MacNeille completions of lattice expansions. (2007). Issue 2. doi:10.1007/s00012-007-2033-1
[34] Igor Walukiewicz. 1995. Completeness of Kozen's Axiomatisation of the Propositional mu-Calculus. In *Proceedings, 10th Annual IEEE Symposium on Logic in Computer Science, San Diego, California, USA, June 26-29, 1995*. IEEE Computer Society, 14–24. doi:10.1109/LICS.1995.523240
[35] Tobias Winkler and Joost-Pieter Katoen. 2023. Certificates for Probabilistic Pushdown Automata via Optimistic Value Iteration. In *TACAS (2) (Lecture Notes in Computer Science, Vol. 13994)*. Springer, 391–409.
[36] Tengshun Yang, Hongfei Fu, Jingyu Ke, Naijun Zhan, and Shiyang Wu. 2024. Piecewise Linear Expectation Analysis via k-Induction for Probabilistic Programs. *CoRR* abs/2403.17567 (2024).

A Omitted Proofs

A.1 Joins and Meets

A.1.1 $\curlyvee$*-Elim and* $\curlywedge$*-Elim.*

$$\frac{a \curlyvee b \preceq c}{b \preceq c}\ \curlyvee\text{-ELIM} \qquad \frac{a \preceq b \curlywedge c}{a \preceq b}\ \curlywedge\text{-ELIM}$$

Consider the following two proofs.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{b \preceq b}\,\text{REFLEX}}{b \preceq b \curlyvee a}\,\curlyvee\text{-INTROR}}{b \preceq a \curlyvee b}\,\curlyvee\text{-COMM} \qquad \dfrac{}{a \curlyvee b \preceq c}\,\text{ASM.}}{b \preceq c}\,\text{TRANS}$$

$$\dfrac{\dfrac{}{a \preceq b \curlywedge c}\,\text{ASM.} \qquad \dfrac{\dfrac{}{b \preceq b}\,\text{REFLEX}}{b \curlyvee c \preceq b}\,\curlywedge\text{-INTROL}}{a \preceq b}\,\text{TRANS}$$

A.2 Shifts

A.2.1 $\bigcirc$*-Over-*$\curlyvee$ *and* $\bigcirc$*-Over-*$\curlywedge$*.*

$$\bigcirc a \curlyvee \bigcirc b \preceq \bigcirc(a \curlyvee b) \qquad \bigcirc(a \curlywedge b) \preceq \bigcirc a \curlywedge \bigcirc b$$

Note, that the other direction is proven semantically. Refer to the proof of soundness in Section A.8.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a \preceq a}\,\text{Reflex}}{a \preceq a \curlyvee b}\,\curlyvee\text{-INTROR}}{\bigcirc a \preceq \bigcirc(a \curlyvee b)}\,\bigcirc\text{-MONO} \qquad \dfrac{\dfrac{\dfrac{}{b \preceq b}\,\text{Reflex}}{b \preceq a \curlyvee b}\,\curlyvee\text{-INTROR}}{\bigcirc b \preceq \bigcirc(a \curlyvee b)}\,\bigcirc\text{-MONO}}{\bigcirc a \curlyvee \bigcirc b \preceq \bigcirc(a \curlyvee b)}\,\curlyvee\text{-INTROL}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a \preceq a}\,\text{Reflex}}{a \curlywedge b \preceq a}\,\curlywedge\text{-INTROL}}{\bigcirc(a \curlywedge b) \preceq \bigcirc a}\,\bigcirc\text{-MONO} \qquad \dfrac{\dfrac{\dfrac{}{b \preceq b}\,\text{Reflex}}{a \curlywedge b \preceq b}\,\curlywedge\text{-INTROL}}{\bigcirc(a \curlywedge b) \preceq \bigcirc b}\,\bigcirc\text{-MONO}}{\bigcirc(a \curlywedge b) \preceq \bigcirc a \curlywedge \bigcirc b}\,\curlywedge\text{-INTROR}$$

A.3 Majora and Minora

A.3.1 $\Diamond$*-IntroR,* $\Box$*-IntroR,* $\Diamond$*-Elim and* $\Box$*-Elim.*

$$\frac{a \preceq b}{a \preceq \Diamond b}\ \Diamond\text{-INTROR} \qquad \frac{\Diamond a \preceq b}{a \preceq b}\ \Diamond\text{-ELIM}$$

$$\frac{a \preceq b}{\Box a \preceq b}\ \Box\text{-INTROL} \qquad \frac{a \preceq \Box b}{a \preceq b}\ \Box\text{-ELIM}$$

For $\Diamond$-INTRO and $\Diamond$-ELIM, consider the following two proofs:

$$\dfrac{\dfrac{}{a \preceq b}\,\text{ASM.} \qquad \dfrac{}{b \preceq \Diamond b}\,\Diamond\text{-INFLATE}}{a \preceq \Diamond b}\,\text{TRANS}$$

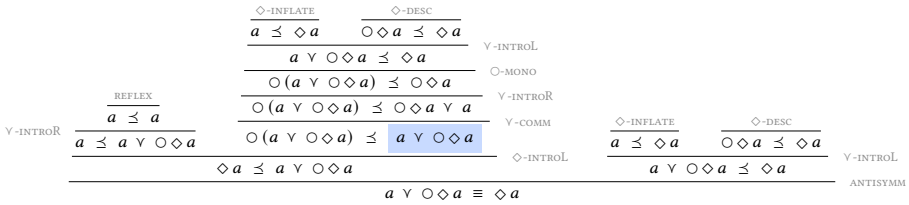


Figure 5: Proof of the expansion rules.

$$\dfrac{\dfrac{}{a \preceq \Diamond a}\,\Diamond\text{-INFLATE} \qquad \dfrac{}{\Diamond a \preceq b}\,\text{ASM.}}{a \preceq b}\,\text{TRANS}$$

For □-INTRO and □-ELIM, consider the following two proofs:

$$\dfrac{\dfrac{}{\Box a \preceq a}\,\Box\text{-DEFLATE} \qquad \dfrac{}{a \preceq b}\,\text{ASM.}}{\Box a \preceq b}\,\text{TRANS}$$

$$\dfrac{\dfrac{}{a \preceq \Box b}\,\text{ASM.} \qquad \dfrac{}{\Box b \preceq b}\,\Box\text{-DEFLATE}}{a \preceq b}\,\text{TRANS}$$

A.3.2 ◇-EXP and □-EXP.

$$\dfrac{}{\Diamond a = a \vee \bigcirc\Diamond a}\,\Diamond\text{-EXP} \qquad \dfrac{}{\Box a = a \wedge \bigcirc\Box a}\,\Box\text{-EXP}$$

The proof of ◇-EXP in in Figure 5.

A.3.3 ◇-INTROL and □-INTROR.

$$\dfrac{a \preceq b \qquad \bigcirc b \preceq b}{\Diamond a \preceq b}\,\Diamond\text{-INTROL}$$

$$\dfrac{a \preceq \bigcirc a \qquad a \preceq b}{a \preceq \Box b}\,\Box\text{-INTROR}$$

Consider the following two proofs.

$$\dfrac{\Diamond\text{-MONO}\ \dfrac{a \preceq b}{\Diamond a \preceq \Diamond b} \qquad \dfrac{\bigcirc b \preceq b}{\Diamond b \preceq b}\,\Diamond\text{-IND}}{\Diamond a \preceq b}\,\text{TRANS}$$

$$\dfrac{\Box\text{-COIND}\ \dfrac{a \preceq \bigcirc a}{a \preceq \Box a} \qquad \dfrac{a \preceq b}{\Box a \preceq \Box b}\,\Box\text{-MONO}}{a \preceq \Box b}\,\text{TRANS}$$

A.4 Flats and Limits

A.4.1 ○-Point.

$$\dfrac{\Diamond a \preceq \Box a}{\bigcirc a \equiv a}\ \bigcirc\text{-FLAT}$$

For the inference from top to bottom, consider the following proof tree:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Diamond a \preceq \Box a}\ \text{ASM.}}{\Diamond a \preceq a}\ \Box\text{-ELIM}}{\bigcirc a \preceq a}\ \bigcirc\text{-IND} \qquad \dfrac{\dfrac{\dfrac{}{\Diamond a \preceq \Box a}\ \text{ASM.}}{a \preceq \Box a}\ \Diamond\text{-ELIM}}{a \preceq \bigcirc a}\ \Box\text{-COIND}}{\bigcirc a \equiv a}\ \text{ANTISYMM}$$

For the converse inference, consider the following:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\bigcirc a = a}\ \text{ASM.}}{\bigcirc a \preceq a}\ \text{WEAKENR}}{\Diamond a \preceq a}\ \bigcirc\text{-IND} \qquad \dfrac{\dfrac{\dfrac{}{\bigcirc a = a}\ \text{ASM.}}{a \preceq \bigcirc a}\ \text{WEAKENR}}{a \preceq \Box a}\ \bigcirc\text{-COIND}}{\Diamond a \preceq \Box a}\ \text{CUT}$$

A.4.2 $\Diamond$ -Asc-Point and $\Box$ -Desc-Point.

$$\dfrac{a \preceq \bigcirc a}{\Diamond\Diamond a \preceq \Box\Diamond a}\ \Diamond\text{-ASC-FLAT} \qquad \dfrac{\bigcirc a \preceq a}{\Diamond\Box a \preceq \Box\Box a}\ \Box\text{-DESC-FLAT}$$

Consider the following proof.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a \preceq \bigcirc a}\ \text{ASM.}}{\Diamond a \preceq \Diamond\bigcirc a}\ \Diamond\text{-MONO}}{\Diamond a \preceq \bigcirc\Diamond a}\ \bigcirc\Diamond\text{-COMM}}{\Diamond a \preceq \Box\Diamond a}\ \Box\text{-COIND}}{\Diamond\Diamond a \preceq \Box\Diamond a}\ \Diamond\text{-IDEM} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\bigcirc a \preceq a}\ \text{ASM.}}{\Box\bigcirc a \preceq \Box a}\ \Box\text{-MONO}}{\bigcirc\Box a \preceq \Box a}\ \bigcirc\Box\text{-COMM}}{\Diamond\Box a \preceq \Box a}\ \Box\text{-COIND}}{\Diamond\Box a \preceq \Box\Box a}\ \Box\text{-IDEM}$$

A.4.3 $\Diamond\Box$ / $\Box\Diamond$-mono.

$$\dfrac{a \preceq b}{\Diamond\Box a \preceq \Box\Diamond b}\ \Diamond\Box\,/\,\Box\Diamond\text{-MONO}$$

Consider the following proof.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a \preceq b}\ \text{ASM.}}{a \preceq \Diamond b}\ \Diamond\text{-INTROR}}{\Box a \preceq \Box\Diamond b}\ \Box\text{-MONO} \qquad \dfrac{\dfrac{\dfrac{}{\bigcirc\Diamond b \preceq \Diamond b}\ \Diamond\text{-DESC}}{\Box\bigcirc\Diamond b \preceq \Box\Diamond b}\ \Box\text{-MONO}}{\bigcirc\Box\Diamond b \preceq \Box\Diamond b}\ \bigcirc\Box\text{-COMM}}{\Diamond\Box a \preceq \Box\Diamond b}\ \Diamond\text{-INTROL}$$

A.5 Functions, Monotonicity, Continuity

A.5.1 semi-cont and semi-cocont.

$$\dfrac{}{\Diamond F a \preceq F \Diamond a}\ \text{SEMI-CONT} \qquad \dfrac{}{F \Box a \preceq \Box F a}\ \text{SEMI-COCONT}$$

We show SEMI-CONT in **??**. Consider the following proof for SEMI-COCONT:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Box a \preceq \bigcirc\Box a}\,\Box\text{-ASC}}{F\Box a \preceq F\bigcirc\Box a}\,F\text{-MONO}}{F\Box a \preceq \bigcirc F\Box a}\,F\bigcirc\text{-COMM} \qquad \dfrac{\dfrac{}{\Box a \preceq a}\,\Box\text{-DEFLATE}}{F\Box a \preceq Fa}\,F\text{-MONO}}{F\Box a \preceq \Box Fa}\,\Box\text{-INTROR}$$

A.6 Iteration

ASC-ITER AND DESC-ITER

$$\dfrac{a \preceq \bigcirc a}{FF^*a \preceq \bigcirc F^*a}\,\text{ASC-ITER} \qquad \dfrac{\bigcirc a \preceq a}{\bigcirc F^*a \preceq FF^*a}\,\text{DESC-ITER}$$

Consider the following proofs.

$$\dfrac{\dfrac{\dfrac{a \preceq \bigcirc a}{F^*a \preceq F^*\bigcirc a}\,F^*\text{-MONO}}{FF^*a \preceq FF^*\bigcirc a}\,F\text{-MONO}}{FF^*a \preceq \bigcirc F^*a}\,\text{ITER} \qquad \dfrac{\dfrac{\dfrac{\bigcirc a \preceq a}{F^*\bigcirc a \preceq F^*a}\,F^*\text{-MONO}}{FF^*\bigcirc a \preceq FF^*a}\,F\text{-MONO}}{\bigcirc F^*a \preceq FF^*a}\,\text{ITER}$$

A.6.1 F^*-INTROL and F^*-INTROR.

$$\dfrac{a \preceq b \qquad Fb \preceq b}{F^*a \preceq b}\,F^*\text{-INTROL}$$

$$\dfrac{a \preceq Fa \qquad a \preceq b}{a \preceq F^*b}\,F^*\text{-INTROR}$$

Consider the following proof.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{a \preceq b}\,\text{ASM.}}{F^*a \preceq F^*b}\,F^*\text{-MONO} \qquad \dfrac{\dfrac{}{Fb \preceq b}\,\text{ASM.}}{F^*b \preceq b}}{F^*a \preceq b}\,F\text{-IND}}{}\,\text{TRANS}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{a \preceq Fa}\,\text{ASM.}}{a \preceq F^*a}\,F\text{-COIND} \qquad \dfrac{\dfrac{}{a \preceq b}\,\text{ASM.}}{F^*a \preceq F^*b}\,F^*\text{-MONO}}{a \preceq F^*b}}{}\,\text{TRANS}$$

A.7 Distribution rules for $\Box$ and $\Diamond$

$\Diamond\vee Dist$ and $\Box\vee Dist$

Proof.

$$\dfrac{\dfrac{\dfrac{}{a \preceq \Diamond a}\,\Diamond\text{-INTROR}}{a \preceq \Diamond a \vee \Diamond b}\,\vee\text{-INTROL} \qquad \dfrac{\dfrac{}{b \preceq \Diamond b}\,\Diamond\text{-INTROR}}{b \preceq \Diamond a \vee \Diamond b}\,\vee\text{-INTROL}}{a \vee b \preceq \Diamond a \vee \Diamond b} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\bigcirc\Diamond a \preceq \Diamond a}\,\Diamond\text{-DESC} \qquad \dfrac{}{\bigcirc\Diamond b \preceq \Diamond b}\,\Diamond\text{-DESC}}{\bigcirc\Diamond a \vee \bigcirc\Diamond b \preceq \Diamond a \vee \Diamond b}\,\vee\text{-INTROL}}{\bigcirc(\Diamond a \vee \Diamond b) \preceq \Diamond a \vee \Diamond b}\,\bigcirc\text{-OVER-}\vee}{\Diamond(a \vee b) \preceq \Diamond a \vee \Diamond b}\,\Diamond\text{-INTROL}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a \preceq a}\,\textsc{reflex}}{a \preceq a \vee b}\,\vee\text{-}\textsc{introR}}{\Diamond a \preceq \Diamond(a \vee b)}\,\Diamond\text{-}\textsc{mono} \qquad \dfrac{\dfrac{\dfrac{}{b \preceq b}\,\textsc{reflex}}{b \preceq a \vee b}\,\vee\text{-}\textsc{introR}}{\Diamond b \preceq \Diamond(a \vee b)}\,\Diamond\text{-}\textsc{mono}}{\Diamond a \vee \Diamond b \preceq \Diamond(a \vee b)}\,\vee\text{-}\textsc{introL}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a \preceq a}\,\textsc{reflex}}{a \preceq a \vee b}\,\vee\text{-}\textsc{introR}}{\Box a \preceq \Box(a \vee b)}\,\Box\text{-}\textsc{mono} \qquad \dfrac{\dfrac{\dfrac{}{b \preceq b}\,\textsc{reflex}}{b \preceq a \vee b}\,\vee\text{-}\textsc{introR}}{\Box b \preceq \Box(a \vee b)}\,\Box\text{-}\textsc{mono}}{\Box a \vee \Box b \preceq \Box(a \vee b)}\,\vee\text{-}\textsc{introL}$$

□

A.8 Soundness of AIC_0

The axiom system AIC_0 is sound for sequence algebras.

We prove the statement by structural induction on the derivation. Let $n \in \mathbb{N}$ be arbitrary but fixed.

Bot and Top.

$$\frac{}{\bot \preceq a}\ \text{BOT} \qquad \frac{}{a \preceq \top}\ \text{TOP}$$

Proof. Both follow directly from the definition of $\top$ and $\bot$.

$$[\![\bot]\!]_n = \bot \sqsubseteq [\![a]\!]_n \qquad \text{(Def } \bot\text{)}$$

$$[\![a]\!]_n \sqsubseteq \top = [\![\top]\!]_n \qquad \text{(Def } \top\text{)}$$

□

$\curlyvee$-comm, $\curlywedge$-comm, $\curlyvee$-assoc and $\curlywedge$-assoc.

$$\frac{}{a \curlyvee b = b \curlyvee a}\ \curlyvee\text{-COMM} \qquad \frac{}{a \curlywedge b = b \curlywedge a}\ \curlywedge\text{-COMM}$$

$$\frac{}{(a \curlyvee b) \curlyvee c = a \curlyvee (b \curlyvee c)}\ \curlyvee\text{-ASSOC} \qquad \frac{}{(a \curlyvee b) \curlyvee c = a \curlyvee (b \curlyvee c)}\ \curlyvee\text{-ASSOC}$$

Proof. Follow directly from the lattice axioms.

$$\begin{aligned}
[\![a]\!]_n \curlyvee [\![b]\!]_n &= \sup\{[\![a]\!]_n, [\![b]\!]_n\} \\
&= [\![b]\!]_n \curlyvee [\![a]\!]_n
\end{aligned}$$

$$\begin{aligned}
[\![a]\!]_n \curlywedge [\![b]\!]_n &= \inf\{[\![a]\!]_n, [\![b]\!]_n\} \\
&= [\![b]\!]_n \curlywedge [\![a]\!]_n
\end{aligned}$$

$$\begin{aligned}
[\![a \curlyvee (b \curlyvee c)]\!]_n &= [\![a]\!]_n \curlyvee ([\![b]\!]_n \curlyvee [\![c]\!]_n) \\
&= ([\![a]\!]_n \curlyvee [\![b]\!]_n) \curlyvee [\![c]\!]_n \\
&= [\![(a \curlyvee b) \curlyvee c]\!]_n
\end{aligned}$$

$$\begin{aligned}
[\![a \curlywedge (b \curlywedge c)]\!]_n &= [\![a]\!]_n \curlywedge ([\![b]\!]_n \curlywedge [\![c]\!]_n) \\
&= ([\![a]\!]_n \curlywedge [\![b]\!]_n) \curlywedge [\![c]\!]_n \\
&= [\![(a \curlywedge b) \curlywedge c]\!]_n
\end{aligned}$$

□

$$\frac{}{a \curlyvee (a \curlywedge b) = a}\ \curlyvee\text{-ABSORB} \qquad \frac{}{a \curlywedge (a \curlyvee b) = a}\ \curlywedge\text{-ABSORB}$$

Proof.

$$\begin{aligned}
[\![a \curlyvee (a \curlywedge b)]\!]_n &= [\![a]\!]_n \curlyvee ([\![a]\!]_n \curlywedge [\![b]\!]_n) \\
&= ([\![a]\!]_n \curlyvee [\![a]\!]_n) \curlywedge ([\![a]\!]_n \curlyvee [\![b]\!]_n) \\
&\preceq [\![(a)]\!]_n
\end{aligned}$$

$$\begin{aligned}
[\![a \curlywedge (a \curlyvee b)]\!]_n &= [\![a]\!]_n \curlywedge ([\![a]\!]_n \curlyvee [\![b]\!]_n) \\
&= ([\![a]\!]_n \curlywedge [\![a]\!]_n) \curlyvee ([\![a]\!]_n \curlywedge [\![b]\!]_n) \\
&\succeq [\![(a)]\!]_n
\end{aligned}$$

The other directions are similar straightforward. □

○-Mono.

$$\frac{a \preceq b}{\bigcirc a \preceq \bigcirc b}\ \bigcirc\text{-MONO}$$

Proof. Assume $a \preceq b$.

$$\begin{aligned}\llbracket \bigcirc a \rrbracket_n &= \llbracket a \rrbracket_{n+1} && \text{(Assumption)}\\ &= \llbracket b \rrbracket_{n+1}\\ &= \llbracket \bigcirc b \rrbracket_n\end{aligned}$$

□

○-of-⊥ and ○-of-⊤.

$$\frac{}{\bigcirc \bot \preceq \bot}\ \bigcirc\text{-OF-}\bot \qquad \frac{}{\top \preceq \bigcirc \top}\ \bigcirc\text{-OF-}\top$$

Proof. Both are direct consequences of the definition of the constants. □

○-Over-∨ and ○-Over-∧.

$$\frac{}{\bigcirc (a \vee b) = \bigcirc a \vee \bigcirc b}\ \bigcirc\text{-OVER-}\vee \qquad \frac{}{\bigcirc (a \wedge b) = \bigcirc a \wedge \bigcirc b}\ \bigcirc\text{-OVER-}\wedge$$

Proof.

$$\begin{aligned}\llbracket \bigcirc (a \vee b) \rrbracket_n = \llbracket a \vee b \rrbracket_{n+1} &= \llbracket a \rrbracket_{n+1} \vee \llbracket b \rrbracket_{n+1}\\ &= \llbracket \bigcirc a \rrbracket_n \vee \llbracket \bigcirc b \rrbracket_n\\ &= \llbracket \bigcirc a \vee \bigcirc b \rrbracket_n\end{aligned}$$

$$\begin{aligned}\llbracket \bigcirc (a \wedge b) \rrbracket_n = \llbracket a \wedge b \rrbracket_{n+1} &= \llbracket a \rrbracket_{n+1} \wedge \llbracket b \rrbracket_{n+1}\\ &= \llbracket \bigcirc a \rrbracket_n \wedge \llbracket \bigcirc b \rrbracket_n\\ &= \llbracket \bigcirc a \wedge \bigcirc b \rrbracket_n\end{aligned}$$

□

◇-Inflate and □-Deflate.

$$\frac{}{a \preceq \Diamond a}\ \Diamond\text{-INFLATE} \qquad \frac{}{\Box a \preceq a}\ \Box\text{-DEFLATE}$$

Proof.

$$\begin{aligned}\llbracket a \rrbracket_n &\sqsubseteq \sup_{n \le k} \llbracket a \rrbracket_k\\ &= \llbracket \Diamond a \rrbracket_n\end{aligned}$$

$$\begin{aligned}\llbracket \Box a \rrbracket_n &= \inf_{n \le k} \llbracket a \rrbracket_k\\ &\sqsubseteq \llbracket a \rrbracket_n\end{aligned}$$

□

◇-Idem and □-Idem. We only need to show one direction of the idempotence rule, since the other is a direct consequence of the inflate/deflate rule.

$$\frac{}{\Diamond \Diamond a = \Diamond a}\ \Diamond\text{-IDEM} \qquad \frac{}{\Box \Box a = \Box a}\ \Box\text{-IDEM}$$

Proof. Note that removing elements from a set can only lower the supremum. Dually, removing elements from a set can only increase the infimum.

$$\begin{aligned}[\![\Diamond \Diamond a]\!]_n &= \sup_{n\le k}[\![\Diamond a]\!]_k = \sup_{n\le k}\sup_{k\le i}[\![a]\!]_i \\ &= \sup_{n\le i}[\![a]\!]_i \\ &= [\![\Diamond a]\!]_n\end{aligned}$$

□-Idem:

$$\begin{aligned}[\![\Box a]\!]_n &= \inf_{n\le k}[\![a]\!]_k \\ &= \inf_{n\le k}\inf_{k\le i}[\![a]\!]_i \\ &= \inf_{n\le k}[\![\Box a]\!]_k = [\![\Box \Box a]\!]_n\end{aligned}$$

□

◇-*Mono and* □-*Mono.*

$$\frac{a \preceq b}{\Diamond a \preceq \Diamond b}\ \Diamond\text{-mono} \qquad \frac{a \preceq b}{\Box a \preceq \Box b}\ \Box\text{-mono}$$

Proof. ◇-Mono: Assume $a \preceq b$. To show that some element is upper bounding a supremum, it is enough to show that every element from the set over which the supremum is formed is upper bounded by the aforementioned element. Thus to prove

$$[\![\Diamond a]\!]_n = \sup_{n\le k}[\![a]\!]_k \sqsubseteq \sup_{n\le k}[\![b]\!]_k = [\![\Diamond b]\!]_n$$

it is enough to show the following for some arbitrary but fixed $i \ge n$:

$$\begin{aligned}[\![a]\!]_i &\sqsubseteq [\![b]\!]_i && \text{(by Assumption)} \\ &\sqsubseteq \sup_{n\le k}[\![b]\!]_k\end{aligned}$$

□-Mono: Assume $a \preceq b$. To show that some element is a lower bound of an infimum, it is enough to show that every element over which we form the infimum is lower bounded by the aforementioned element. Thus to prove

$$[\![\Box a]\!]_n = \inf_{n\le k}[\![a]\!]_k \sqsubseteq \inf_{n\le k}[\![b]\!]_k = [\![\Box b]\!]_n$$

it is enough to show for some arbitrary $i \ge n$

$$\begin{aligned}\inf_{n\le k}[\![a]\!]_k &\sqsubseteq [\![a]\!]_i \\ &\sqsubseteq [\![b]\!]_i && \text{(by Assumption)}\end{aligned}$$

□

◇○ -*Comm and* □○ -*Comm.*

$$\frac{}{\bigcirc\Diamond a = \Diamond\bigcirc a}\ \bigcirc\Diamond\text{-comm} \qquad \frac{}{\bigcirc\Box a = \Box\bigcirc a}\ \bigcirc\Box\text{-comm}$$

Proof.

$$\begin{aligned}[\![\bigcirc \Diamond a]\!]_n = [\![\Diamond a]\!]_{n+1} &= \sup_{n+1\le k}[\![a]\!]_k \\ &= \sup_{n\le k}[\![a]\!]_{k+1} \\ &= \sup_{n\le k}[\![\bigcirc a]\!]_k = [\![\Diamond \bigcirc a]\!]_n \\ [\![\bigcirc \Box a]\!]_n = [\![\Box a]\!]_{n+1} &= \inf_{n+1\le k}[\![a]\!]_k \\ &= \inf_{n\le k}[\![a]\!]_{k+1} \\ &= \inf_{n\le k}[\![\bigcirc a]\!]_k = [\![\Box \bigcirc a]\!]_n\end{aligned}$$

□

◇-Ind and □-CoInd.

$$\frac{\bigcirc a \preceq a}{\Diamond a \preceq a}\ \Diamond\text{-IND}$$

Validity of ◇-ind for Sequence Algebras. From top to bottom, assume that $\bigcirc a \preceq a$, i.e.

$$[\![\bigcirc a]\!]_n \overset{\text{Table 2}}{=} [\![a]\!]_{n+1} \sqsubseteq [\![a]\!]_n \tag{†}$$

for all n. This premise enables us to prove the conclusion of ◇-ind: First, notice that

$$\begin{aligned} \Diamond a \preceq a \quad &\text{iff} \quad \forall n\colon \sup_{n \le k} [\![a]\!]_k \sqsubseteq [\![a]\!]_n \\ &\text{iff} \quad \forall n, j\colon [\![a]\!]_{n+j} \sqsubseteq [\![a]\!]_n \end{aligned}$$

by definition of suprema. Now let n be arbitrary but fixed. We prove that the latter statement holds by induction on j. The base case $j = 0$ is trivial. For the induction step, we have

$$[\![a]\!]_{n+j+1} \overset{(\dagger)}{\sqsubseteq} [\![a]\!]_{n+j} \overset{\text{I.H.}}{\sqsubseteq} [\![a]\!]_n\ .$$

From bottom to top, assume $\Diamond a \preceq a$, i.e. $[\![\Diamond a]\!]_n \sqsubseteq [\![a]\!]_n$. Then

$$\begin{aligned} [\![\bigcirc a]\!]_n \overset{\text{Table 2}}{=} [\![a]\!]_{n+1} &\overset{\text{choose } k = n+1}{\sqsubseteq} \sup_{n \le k} [\![a]\!]_k \\ &\overset{\text{Table 2}}{=} [\![\Diamond a]\!]_n \overset{\text{by assumption}}{\sqsubseteq} [\![a]\!]_n\ . \end{aligned}$$

□

$$\frac{a \preceq \bigcirc a}{a \preceq \Box a}\ \Box\text{-COIND}$$

Proof. We show both directions seperatly. Assume $a \preceq \bigcirc a$, i.e. a is an ascending chain.

$$[\![a]\!]_0 \sqsubseteq [\![a]\!]_1 \sqsubseteq [\![a]\!]_2 \sqsubseteq [\![a]\!]_3 \sqsubseteq \dots,$$

But then $\Box a \succeq a$, since

$$\begin{aligned} [\![\Box a]\!]_n &= \inf_{n \le k} [\![a]\!]_k \\ &= [\![a]\!]_n \qquad (a \text{ is an asc. chain}) \end{aligned}$$

Conversely, we assume $a \preceq \Box a$, i.e.

$$[\![a]\!]_n \sqsubseteq [\![\Box a]\!]_n\ .$$

Then

$$\begin{aligned} [\![\bigcirc a]\!]_n &= [\![a]\!]_{n+1} \\ &\sqsupseteq \inf_{n \le k} [\![a]\!]_k \\ &= [\![\Box a]\!]_n \\ &\sqsupseteq [\![a]\!]_n \end{aligned}$$

□

F○ -Comm and Iter.

$$\frac{}{F \bigcirc a = \bigcirc F a}\ F\bigcirc\text{-COMM}$$

$$[\![\bigcirc Fa]\!]_n = [\![Fa]\!]_{n+1} = F[\![a]\!]_{n+1} = F[\![\bigcirc a]\!]_n = [\![F\bigcirc a]\!]_n$$

$$\frac{}{\bigcirc F^* a = F F^* \bigcirc a}\ \text{ITER}$$

$$\begin{aligned}\llbracket \bigcirc F^* a \rrbracket_n &= \llbracket F^* a \rrbracket_{n+1} = F^{n+1} \llbracket a \rrbracket_{n+1} \\ &= F^{n+1} \llbracket \bigcirc a \rrbracket_n \\ &= F \llbracket F^* a \rrbracket_n = \llbracket F F^* \bigcirc a \rrbracket_n\end{aligned}$$

FF^*-Comm.

$$\frac{}{F F^* a = F^* F a}\ FF^*\text{-comm}$$

$$\begin{aligned}\llbracket F F^* a \rrbracket_n &= F \llbracket F^* a \rrbracket_n = F F^n \llbracket a \rrbracket_n \\ &= F^n \llbracket F a \rrbracket_n = \llbracket F^* F a \rrbracket_n\end{aligned}$$

F^*-Ind and F^*-CoInd.

$$\frac{F a \preceq a}{F^* a \preceq a}\ F\text{-ind}$$

Assume F to be monotone and $F a \preceq a$. We need to show $\llbracket F^* a \rrbracket_n \sqsubseteq \llbracket a \rrbracket_n$. By definition, this claim is equivalent to $F^n \llbracket a \rrbracket_n \sqsubseteq \llbracket a \rrbracket_n$. We prove the strengthened version with an arbitrary but fixed m:

$$F^n \llbracket a \rrbracket_m \sqsubseteq \llbracket a \rrbracket_m$$

By induction on n, assume the following induction hypothesis (the base case follows directly by Reflexivity):

$$F^{n-1} \llbracket a \rrbracket_m \sqsubseteq \llbracket a \rrbracket_m \tag{IH}$$

We show $F^n \llbracket a \rrbracket_m \sqsubseteq \llbracket a \rrbracket_m$. Using transitivity, it is enough to prove $F^n \llbracket a \rrbracket_m \sqsubseteq F^{n-1} \llbracket a \rrbracket_m$ and $F^{n-1} \llbracket a \rrbracket_m \sqsubseteq \llbracket a \rrbracket_m$. The second claim follows directly with IH.

For the first claim, it is sufficient to show for an arbitrary index k that $F^k \llbracket a \rrbracket_m \sqsubseteq F^{k-1} \llbracket a \rrbracket_m$. We use induction on k. While the base case for $k = 0$ follows directly from the assumption $F a \preceq a$, consider the following for the induction step: Assume the induction hypothesis $F^{k-1} \llbracket a \rrbracket_m \sqsubseteq F^{k-2} \llbracket a \rrbracket_m$. We prove:

$$F^k \llbracket a \rrbracket_m \sqsubseteq F^{k-1} \llbracket a \rrbracket_m$$

Since F is monotone, it is enough to show $F^{k-1} \llbracket a \rrbracket_m \sqsubseteq F^{k-2} \llbracket a \rrbracket_m$, which is exactly the induction hypothesis.

$$\frac{a \preceq F a}{a \preceq F^* a}\ F\text{-coind}$$

Assume F to be monotone and $a \preceq F a$. We need to show $\llbracket a \rrbracket_n \sqsubseteq \llbracket F^* a \rrbracket_n$. By definition, this claim is equivalent to $\llbracket a \rrbracket_n \sqsubseteq F^n \llbracket a \rrbracket_n$. We prove the strengthened version with an arbitrary but fixed m:

$$\llbracket a \rrbracket_m \sqsubseteq F^n \llbracket a \rrbracket_m$$

By induction on n, assume the following induction hypothesis (the base case follows directly by Reflexivity):

$$\llbracket a \rrbracket_m \sqsubseteq F^{n-1} \llbracket a \rrbracket_m \tag{IH}$$

We show $\llbracket a \rrbracket_m \sqsubseteq F^n \llbracket a \rrbracket_m$. Using transitivity, it is enough to prove $F^{n-1} \llbracket a \rrbracket_m \sqsubseteq F^n \llbracket a \rrbracket_m$ and $\llbracket a \rrbracket_m \sqsubseteq F^{n-1} \llbracket a \rrbracket_m$. The second claim follows directly with IH.

For the first claim, it is sufficient to show that for an arbitrary index k $F^{k-1} \llbracket a \rrbracket_m \sqsubseteq F^k \llbracket a \rrbracket_m$. We use induction for k. While the base case $k = 0$ follows directly from the assumption $a \preceq F a$, consider the following for the induction step: Assume the induction hypothesis $F^{k-2} \llbracket a \rrbracket_m \sqsubseteq F^{k-1} \llbracket a \rrbracket_m$. We show:

$$F^{k-1} \llbracket a \rrbracket_m \sqsubseteq F^k \llbracket a \rrbracket_m$$

Since F is monotone, it is enough to show $F^{k-2} \llbracket a \rrbracket_m \sqsubseteq F^{k-1} \llbracket a \rrbracket_m$, which is exactly the induction hypothesis.

A.9 Additional Proofs

A.9.1 *Depth collapse.*

Theorem 23 (Majora/Minora Alternation Depth Collapse). *The majora/minora alternation depth hierarchy in iteration logic collapses at level 2, i.e. for any formula a, the equivalences*

$$\mathsf{M}_1\,\mathsf{M}_2\,\cdots\,\mathsf{M}_k\,\Diamond\,\Diamond\,\cdots\,\Diamond\,\Box\,\Box\,\cdots\,\Box\,a \quad\equiv\quad \Diamond\,\Box\,a \qquad \text{and}$$
$$\mathsf{M}_1\,\mathsf{M}_2\,\cdots\,\mathsf{M}_k\,\Box\,\Box\,\cdots\,\Box\,\Diamond\,\Diamond\,\cdots\,\Diamond\,a \quad\equiv\quad \Box\,\Diamond\,a$$

hold, where the leading $\mathsf{M}_1\,\cdots\,\mathsf{M}_k$ *are any sequence of* $\Diamond$*'s and* $\Box$*'s.*

Proof Sketch. We only prove the first equivalence; the other one is analogous. Let $b = \mathsf{M}_1\,\mathsf{M}_2\,\cdots\,\mathsf{M}_k\,\Diamond\,\Diamond\,\cdots\,\Diamond\,\Box\,\Box\,\cdots\,\Box\,a$. First, by repeatedly applying $\Diamond$-idem and $\Box$-idem, we can bring b into an alternation normal form $\mathsf{M}_1\,\mathsf{M}_2\,\cdots\,\mathsf{M}_\ell\,\Diamond\,\Box\,a$.

Consider now the innermost subformula $\mathsf{M}_\ell\,\Diamond\,\Box\,a$. If $\mathsf{M}_\ell = \Diamond$, then we can again apply $\Diamond$-idem to obtain the equivalent formula $\Diamond\,\Box\,a$. If $\mathsf{M}_\ell = \Box$, we can use the fact that $\Box$ does not affect flats and again obtain the equivalent formula $\Diamond\,\Box\,a$.

Consider the following:

$$\dfrac{\dfrac{}{\Box\,\Diamond\,\Box\,a \preceq \Diamond\,\Box\,a}\,\Box\text{-deflate} \qquad \dfrac{\dfrac{}{\Diamond\,\Diamond\,\Box\,a \preceq \Box\,\Diamond\,\Box\,a}\,\Diamond\Box\text{-flat}}{\Diamond\,\Box\,a \preceq \Box\,\Diamond\,\Box\,a}\,\Diamond\text{-idem}}{\Box\,\Diamond\,\Box\,a \equiv \Diamond\,\Box\,a}\,\text{antisymm}$$

So in any case we could show that $\mathsf{M}_\ell\,\Diamond\,\Box\,a \equiv \Diamond\,\Box\,a$. Repeatedly applying this proof procedure to $\mathsf{M}_{\ell-1}$ till M_1 finally leaves us with the desired $\Diamond\,\Box\,a \equiv b$. □

A.9.2 *FMono iff monotone.*

$$\dfrac{a \preceq b}{F\,a \preceq F\,b}\;F\text{-mono}$$

Proof. Assume FMono is admissible, i.e. if

$$\forall n : [\![a]\!]_n \preceq [\![b]\!]_n$$

then

$$\forall n : [\![Fa]\!]_n \preceq [\![Gb]\!]_n$$

for arbitrary a and b. Let n be arbitrary but fixed, we show that F is a monotone function. Given two lattice elements x, y, we show that if $x \sqsubseteq y$, then $Fx \sqsubseteq Fy$. Take the constant sequence of x and y in Iteration Logic. The claim follows directly from the assumptions at every possible step in the sequence.

For the other direction, let F be a monotone function. Assume $a \preceq b$, for arbitrary n the following follows:

$$\begin{aligned} [\![Fa]\!]_n &= F[\![a]\!]_n \\ &\sqsubseteq F[\![b]\!]_n && \text{(Monotonicity)} \\ &= [\![Fb]\!]_n \end{aligned}$$

□

A.9.3 *F^*-mono is admissible, if F-mono is admissible.*

$$\dfrac{a \preceq b}{F^*\,a \preceq F^*\,b}\;F^*\text{-mono}$$

Proof. Assume F-mono is admissible. We show that for an arbitrary n the following holds

$$F^n[\![a]\!]_n \sqsubseteq F^n[\![b]\!]_n$$

assuming $\forall m : [\![a]\!]_m \sqsubseteq [\![b]\!]_m$.

It is enough to show the following:

$$\forall k : F^k[\![a]\!]_n \sqsubseteq F^k[\![b]\!]_n$$

We prove the claim by induction on k, the base case follows directly from the assumption. Consider the induction hypothesis $F^k[\![a]\!]_n \sqsubseteq F^k[\![b]\!]_n$, we show:

$$F^{k+1}[\![a]\!]_n \sqsubseteq F^{k+1}[\![b]\!]_n$$

Using F-MONO, it suffices to show:

$$F^k[\![a]\!]_n \sqsubseteq F^k[\![b]\!]_n$$

which is exactly the induction hypothesis. □

A.9.4 ω-CONT is admissible iff F is omega-continuous.

$$\frac{a \preceq \bigcirc a}{F \Diamond a \preceq \Diamond F a}\ \omega\text{-CONT}$$

PROOF. We first show the if-direction. Assume F is omega-continuous and a is an ascending chain. Thus $[\![a]\!]_n$ is a monotonically increasing sequence. Let n be arbitrary but fixed.

$$\begin{aligned}
[\![F\Diamond a]\!]_n = F[\![\Diamond a]\!]_n &= F \sup_{n\le m} [\![a]\!]_n \\
&\sqsubseteq \sup_{n\le m} F[\![a]\!]_n && \text{(Assumption)} \\
&= \sup_{n\le m} [\![Fa]\!]_n \\
&= [\![\Diamond Fa]\!]_n
\end{aligned}$$

For the other direction, assume ω-CONT is admissible, i.e.

$$\forall n : [\![F\Diamond a]\!]_n \preceq [\![\Diamond Fa]\!]_n$$

for an ascending chain a. We show F is omega-continuous, i.e.

$$F \sup_{m\ge n} s_m \sqsubseteq \sup_{m\ge n} Fs_m$$

for a monotonically increasing sequence s.

Let a be a ascending chain and take $[\![a]\!]_m = s_m$. Since a is an ascending chain, s is monotonically increasing.

$$\begin{aligned}
F \sup_{m\ge n} s_m = F \sup_{m\ge n} [\![a]\!]_m &= F[\![\Diamond a]\!]_n \\
&= [\![F\Diamond a]\!]_n \\
&\sqsubseteq [\![\Diamond Fa]\!]_n && \text{(Assumption)} \\
&= \sup_{m\ge n} [\![Fa]\!]_m \\
&= \sup_{m\ge n} F[\![a]\!]_m = \sup_{m\ge n} Fs_m
\end{aligned}$$

□

A.9.5 ω-COCONT is admissible iff F is omega-cocontinuous.

$$\frac{\bigcirc a \preceq a}{\Box F a \preceq F \Box a}\ \omega\text{-COCONT}$$

PROOF. We first show the if-direction. Assume F is omega-cocontinuous and a is an descending chain. Thus $[\![a]\!]_n$ is a monotonically decreasing sequence. Let n be arbitrary but fixed.

$$\begin{aligned}
[\![\Box Fa]\!]_n = \inf_{n\le m} [\![Fa]\!]_n &= \inf_{n\le m} F[\![a]\!]_n \\
&\sqsubseteq F \inf_{n\le m} [\![a]\!]_n && \text{(Assumption)} \\
&= F[\![\Box a]\!]_n \\
&= [\![F\Box a]\!]_n
\end{aligned}$$

$$\frac{}{G_b^{k+1} b \preceq G_b^k b}\ G_b^k\text{-DEFLATE} \qquad \frac{}{G_b^k b \preceq b}\ G_b^k\text{-BELOW}$$

$$\frac{F G_b^k b \preceq b}{F G_b^k b \preceq G_b^k b}\ k\text{-IND-PARK}$$

$$\frac{\bigcirc b \preceq b}{\bigcirc G_b^k b \preceq G_b^k b}\ G_b^k\text{-ASC-PRES}$$

Figure 6: Additional lemmas required for proving k-IND (cf. Section 4.3).

For the fi-direction, assume ω-COCONT is admissible, i.e.

$$\forall n : [\![\Box Fa]\!]_n \preceq [\![F\Box a]\!]_n$$

for an descending chain a. We show F is omega-cocontinuous, i.e.

$$\inf_{m\geq n} Fs_m \sqsubseteq F \inf_{m\geq n} s_m$$

for a monotonically decreasing sequence s. Let a be a descending chain and take $[\![a]\!]_m = s_m$. Since a is a descending chain, s is an monotonically decreasing sequence.

$$\begin{aligned}
\inf_{m\geq n} Fs_m = \inf_{m\geq n} F[\![a]\!]_m &= \inf_{m\geq n} [\![Fa]\!]_n \\
&= [\![\Box Fa]\!]_n \\
&\sqsubseteq [\![F\Box a]\!]_n && \text{(Assumption)} \\
&= F[\![\Box a]\!]_m \\
&= F \inf_{m\geq n} [\![a]\!]_m = F \inf_{m\geq n} Fs_m
\end{aligned}$$

□

A.9.6 c-CONT and c-COCONT are admissible iff F is countably-(co)continuous.

$$\frac{}{F \Diamond a \preceq \Diamond F a}\ \text{c-CONT} \qquad \frac{}{\Box F a \preceq F \Box a}\ \text{c-COCONT}$$

The proof follows analogous to the proofs for omega-cocontinuity, except that we do not restrict ourselves on monotonically increases and decreasing sequences.

A.10 Appendix to Section 4.2

Proof of Theorem 14. We prove Theorem 14.(2).Suppose that F is ω-cocontinuous and $\ell \in L$. Then $\inf_{n\in\omega} \sup_{k\geq n} F^k(\ell)$ is a postfixed point of F as shown by the following computation:

$$\begin{aligned}
F\left(\inf_{n\in\omega} \sup_{k\geq n} F^k(\ell)\right) &= \inf_{n\in\omega} F\left(\sup_{k\geq n} F^k(\ell)\right) && \text{(by } F \text{ } \omega\text{-cocont.)} \\
&\sqsupseteq \inf_{n\in\omega} \sup_{k\geq n} F\left(F^k(\ell)\right) && \text{(by } F \text{ semi-cont.)} \\
&= \inf_{n\in\omega} \sup_{k\geq n} F^{k+1}(\ell) \\
&= \inf_{n} \sup_{k\geq n} F^k(\ell)
\end{aligned}$$

For the last step, observe that the sequences $(\sup_{k\geq n} F^k(\ell))_{n\in\omega}$ and $(\sup_{k\geq n} F^{k+1})_{n\in\omega}$ are both non-increasing, and the latter is a subsequence the former, so they have the same infimum. □

A.11 Appendix to Section 4.3

First recall that in the definition of the k-induction operator

$$G_b^k b = \begin{cases} b & \text{if } k = 0 \\ F G_b^{k-1} b \wedge b & \text{otherwise .} \end{cases}$$

we mean to define *syntactic* equality of terms, so e.g. defining that $G_b^2\, b$ is a name for the term $F\, G_b^1\, b \wedge b$. To keep proof trees concise, we will often apply the INDISCERN rule for replacing, e.g. s by s' without explicitly mentioning the obvious (semantic) equivalence of s and s'. For our proof, we require a few auxiliary lemmas (shown in Section A.11): We need that applying G_b^k once more to b takes us down in the partial order (G_b^k-DEFLATE). This in turn implies that $G_b^k\, b \preceq b$ (G_b^k-BELOW). For a derivation, see Section A.11.1. As third auxiliary lemma, we need that if $F\, G_b^k\, b$ is below b, then $F\, G_b^k\, b$ is even below $G_b^k\, b$ (k-IND-PARK). We prove this in Section A.11.3. Finally, we require the rule G_b^k-ASC-PRES, which we prove in Section A.11.2. Now, k-IND for $k = 0$ is an immediate instance of Theorem 13. For $k \geq 1$, we employ the preceding lemmas, resulting in the proof shown in Section A.11.4.

A.11.1 G_b^k*-DEFLATE.* By inudction on k. For $k = 0$, we have:

$$\dfrac{\dfrac{\dfrac{}{b \preceq b}\,\text{REFLEX}}{F\, G_b^0\, b \wedge b \preceq b}\,\wedge\text{-INTROL}}{F\, G_b^0\, b \wedge b \preceq G_b^0\, b}\,\text{INDISCERN}}{G_b^1\, b \preceq G_b^0\, b}\,\text{INDISCERN}$$

For the induction step, assume the admissibility of G_b^k-DEFLATE for some arbitrary, but fixed, $k \geq 1$ and consider the following:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{G_b^k\, b \preceq G_b^{k-1}\, b}\,\text{I.H.}}{F\, G_b^k\, b \preceq F\, G_b^{k-1}\, b}\,F\text{-MONO}}{b \wedge F\, G_b^k\, b \preceq F\, G_b^{k-1}\, b}\,\wedge\text{-INTROL}}{F\, G_b^k\, b \wedge b \preceq F\, G_b^{k-1}\, b}\,\wedge\text{-COMM}}{G_b^{k+1}\, b \preceq F\, G_b^{k-1}\, b}\,\text{INDISCERN} \qquad \dfrac{\dfrac{\dfrac{}{b \preceq b}\,\text{REFLEX}}{F\, G_b^k\, b \wedge b \preceq b}\,\wedge\text{-INTROL}}{G_b^{k+1}\, b \preceq b}\,\text{INDISCERN}}{G_b^{k+1}\, b \preceq F\, G_b^{k-1}\, b \wedge b}\,\wedge\text{-INTROR}}{G_b^{k+1}\, b \preceq G_b^k\, b}\,\text{INDISCERN}$$

A.11.2 Proof of G_b^k *-ASC-PRES.* By induction on k. The base case $k = 0$ is trivial. For the induction step, we have:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\bigcirc G_b^k\, b \preceq G_b^k\, b}\,\text{I.H.}}{F \bigcirc G_b^k\, b \preceq F\, G_b^k\, b}\,F\text{-MONO}}{\bigcirc F\, G_b^k\, b \preceq F\, G_b^k\, b}\,F\bigcirc\text{-COMM}}{\bigcirc F\, G_b^k\, b \wedge \bigcirc b \preceq F\, G_b^k\, b}\,\wedge\text{-INTROL} \qquad \dfrac{\dfrac{}{\bigcirc b \preceq b}\,\text{ASM.}}{\bigcirc F\, G_b^k\, b \wedge \bigcirc b \preceq b}\,\wedge\text{-INTROL}}{\bigcirc F\, G_b^k\, b \wedge \bigcirc b \preceq F\, G_b^k\, b \wedge b}\,\wedge\text{-INTROR}}{\bigcirc (F\, G_b^k\, b \wedge b) \preceq F\, G_b^k\, b \wedge b}\,\bigcirc\text{-OVER-}\wedge}{\bigcirc\, G_b^{k+1}\, b \preceq G_b^{k+1}\, b}\,\text{INDISCERN}$$

A.11.3 Proof of Third Auxiliary Lemma. By induction on k. The base case $k = 0$ is trivial. For the induction step with $k \geq 1$, we have:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{G_b^k\, b \preceq G_b^{k-1}\, b}\,G_b^k\text{-DEFLATE}}{F\, G_b^k\, b \preceq F\, G_b^{k-1}\, b}\,F\text{-MONO} \qquad \dfrac{}{F\, G_b^k\, b \preceq b}\,\text{ASM.}}{F\, G_b^k\, b \preceq F\, G_b^{k-1}\, b \wedge b}\,\wedge\text{-INTROR}}{F\, G_b^k\, b \preceq G_b^k\, b}\,\text{INDISCERN}$$

A.11.4 Proof of k*-IND.* The case $k = 0$ is trivial. For $k \geq 1$, we have:

$$\dfrac{\dfrac{}{\bot \preceq G_b^k\, b}\,\text{BOT} \qquad \dfrac{\dfrac{}{F\, G_b^k\, b \preceq b}\,\text{ASM.}}{F\, G_b^k\, b \preceq G_b^k\, b}\,k\text{-IND-PARK} \qquad \dfrac{\dfrac{}{\bigcirc b \preceq b}\,\text{ASM.}}{\bigcirc G_b^k\, b \preceq G_b^k\, b}\,G_b^k\text{-ASC-PRES} \qquad \dfrac{}{G_b^k\, b \preceq b}\,G_b^k\text{-BELOW}}{\dfrac{\Diamond F^* \bot \preceq G_b^k\, b}{\Diamond F^* \bot \preceq b}\,\text{TRANS}}\,\text{TKP-LEAST}$$

□

A.12 Appendix to Section 6.1

We give a detailed account of Theorem 18, which states that the finitary quasiequational theory of the operators ⊚ and ○ on sequences has no finite axiomatization.

A.12.1 Finitary Quasiequations in General. We first recall some standard terminology and notation from universal algebra, generalizing the concepts introduced in Section 2 from sequence algebras to algebras over any finitary signature.

Notation 24. Fix a finitary algebraic signature Σ, i.e. a set of operation symbols with associated finite arities. Moreover, fix a countably infinite set

$$\mathrm{Vars} = \{x, y, z, \ldots\}$$

of variables, and let $\Sigma^*\mathrm{Vars}$ denote the set of Σ-terms formed over the set Vars of variables. A Σ-algebra is a set A equipped with an operation $\mathsf{f}^A \colon A^n \to A$ for every n-ary operation symbol in Σ. Given a Σ-algebra A, a variable interpretation $\mathfrak{I} \colon \mathrm{Vars} \to A$ and a term $t \in \Sigma^*\mathrm{Vars}$, we write ${}^{\mathfrak{I}}[\![t]\!] \in A$ for the value of the term t in the algebra A under the given interpretation. Formally, ${}^{\mathfrak{I}}[\![t]\!]$ is defined inductively by

$${}^{\mathfrak{I}}[\![x]\!] = \mathfrak{I}(x) \qquad \text{and} \qquad {}^{\mathfrak{I}}[\![\mathsf{f}(t_1, \ldots, t_n)]\!] = \mathsf{f}^A({}^{\mathfrak{I}}[\![t_1]\!], \ldots, {}^{\mathfrak{I}}[\![t_n]\!])$$

where $x \in \mathcal{V}$, f is an n-ary operation symbol from Σ, and $t_1, \ldots, t_n \in \Sigma^*\mathcal{V}$. Finally, given a substitution (a map $\sigma \colon \mathrm{Vars} \to \Sigma^*\mathrm{Vars}$) and a term $t \in \Sigma^*\mathrm{Vars}$, we write $t[\sigma] \in \Sigma^*\mathrm{Vars}$ for the term obtained by applying the substitution σ to the variables of t. Formally,

Definition 25. (1) A *(Σ-)identity* is an expression of the form

$$s = t \qquad \text{where } s, t \in \Sigma^*\mathrm{Vars}.$$

A *(finitary Σ-)quasiequation* is an expression of the form

$$P \Longrightarrow s = t \tag{A.1}$$

where $s = t$ is an identity and P is a finite set of identities. The quasiequation (A.1) is *satisfied* in a Σ-algebra A if for every variable interpretation $\mathfrak{I} \colon \mathrm{Vars} \to A$,

$${}^{\mathfrak{I}}[\![u]\!] = {}^{\mathfrak{I}}[\![v]\!] \text{ for all } u = v \text{ in } P \quad \Longrightarrow \quad {}^{\mathfrak{I}}[\![s]\!] = {}^{\mathfrak{I}}[\![t]\!]. \tag{A.2}$$

(2) The *substitution instance* of (A.1) for a substitution σ is the finitary quasiequation

$$P[\sigma] \Longrightarrow s[\sigma] = t[\sigma] \qquad \text{where } P[\sigma] = \{u[\sigma] = v[\sigma] \mid (u = v) \in P\}.$$

Notation 26. We commonly write

$$s_1 = t_1 \ \wedge \ \ldots, \wedge s_n = t_n \Longrightarrow s = t$$

or simply

$$s_1 = t_1, \ \ldots, \ s_n = t_n \Longrightarrow s = t$$

for a quasiequation

$$\{s_1 = t_1, \ \ldots, \ s_n = t_n\} \Longrightarrow s = t$$

This notation allows to freely permute or duplicate premises.

Example 27. We denote by $\mathsf{Ax}_=$ the following set of quasiequations, where f ranges over operations in Σ and n is the arity of f.

$$\Longrightarrow x = x \tag{A.3}$$

$$x = y \Longrightarrow y = z \tag{A.4}$$

$$x = y, \ y = z \Longrightarrow x = z \tag{A.5}$$

$$x_1 = y_1, \ \ldots \ x_n = y_n \Longrightarrow \mathsf{f}(x_1, \ldots, x_n) = \mathsf{f}(y_1, \ldots, y_n) \tag{A.6}$$

These correspond to axioms of standard equational logic; in particular, they hold in every Σ-algebra.

Remark 28. If a quasiequation is satisfied in an algebra A, then so are all its substitution instances.

Definition 29. Given a set Ax of finitary quasiequations, a *proof* of a finitary quasiequation

$$P \Longrightarrow s = t$$

from Ax is a finite tree with the following properties:

(1) Every node is labelled with some identity $u = v$ where $u, v \in \Sigma^*\mathsf{Vars}$.
(2) The root is labelled with $s = t$.
(3) For every inner node labelled $u = v$ with children labelled $u_1 = v_1, \dots, u_n = v_n$, the quasiequation

$$u_1 = v_1, \dots, u_n = v_n \Longrightarrow u = v$$

is a substitution instance of some quasiequation in $\mathsf{Ax} \cup \mathsf{Ax}_=$.
(4) For every leaf node, the label $u = v$ is either an identity in P or a substitution instance of some premise-free quasiequation in $\mathsf{Ax} \cup \mathsf{Ax}_=$.

A quasiequation $P \Longrightarrow s = t$ is Ax-*provable*, denoted

$$\mathsf{Ax} \vdash P \Longrightarrow s = t,$$

if there exists a proof of it from Ax. It is *provable in equational logic* if it is $\emptyset$-provable, denoted

$$\vdash P \Longrightarrow s = t.$$

Remark 30. If $\mathsf{Ax} \vdash P \Longrightarrow s = t$, then every $\mathsf{Ax} \cup \{P \Longrightarrow s = t\}$-provable quasiequation is Ax-provable. In other words, one can treat quasiequations provable from Ax like additional axioms. Indeed, any use of a substitution instance $P[\sigma] \Longrightarrow s[\sigma] = t[\sigma]$ in a proof from $\mathsf{Ax} \cup \{P \Longrightarrow s = t\}$ can be replaced with a proof of $P[\sigma] \Longrightarrow s[\sigma] = t[\sigma]$ from Ax.

A.12.2 Discrete Stream Algebras.

Definition 31. A *discrete sequence algebra* is given by the set A^ω of sequences over a set A equipped with the unary operations

$$\circledcirc : A^\omega \to A^\omega, \qquad \circledcirc\,(\varphi) = (\varphi(0), \varphi(0), \varphi(0), \dots),$$

and

$$\bigcirc : A^\omega \to A^\omega, \qquad \bigcirc\,(\varphi) = (\varphi(1), \varphi(2), \varphi(3), \dots).$$

Note that discrete sequence algebras are algebras for the algebraic signature Δ given by the unary operation symbols $\circledcirc$ and $\bigcirc$:

$$\Delta = \{\circledcirc : 1, \bigcirc : 1\}.$$

Definition 32. (1) A $\bigcirc$*-term* term is a term of the form $\bigcirc^k(x)$, where $k \geq 0$ and $x \in \mathsf{Vars}$.
(2) A $\bigcirc$*-identity* is an identity $s = t$ between $\bigcirc$-terms.
(3) A $\circledcirc\bigcirc$*-term* term is a term of the form $\circledcirc\bigcirc^k(x)$, where $k \geq 0$ and $x \in \mathsf{Vars}$.
(4) A $\circledcirc\bigcirc$*-identity* is an identity $s = t$ between $\circledcirc\bigcirc$-terms.
(5) A *homogeneous identity* is either a $\bigcirc$-identity or a $\circledcirc\bigcirc$-identity.

Definition 33. A finitary Δ-quasiequation is *valid for discrete sequence algebras* if it satisfied in every discrete sequence algebra.

In the remainder of Section A.12, by a *quasiequation* we always mean a finitary Δ-quasiequation, and by a *valid quasiequation* we mean one that is valid for discrete sequence algebras.

Example 34. The following quasiequations are valid:

$$\Longrightarrow \circledcirc\,(x) = \circledcirc^2(x) \tag{A.7}$$

$$\Longrightarrow \bigcirc\circledcirc\,(x) = \circledcirc\,(x) \tag{A.8}$$

$$x = \circledcirc\,(y) \Longrightarrow \circledcirc\,(x) = \circledcirc\,(y) \tag{A.9}$$

$$x = \circledcirc\,(y) \Longrightarrow \bigcirc\,(x) = x \tag{A.10}$$

Remark 35. If Ax is a set of valid quasiequations, then every Ax-provable quasiequation is valid. This is immediate from Remark 28 by induction on the height of proof trees.

We start with a few technical results on quasiequations provable in equational logic.

Lemma 36. *If $\vdash P \Longrightarrow s = t$ and all identities in P are homogeneous, then*
(1) *s is a $\bigcirc$-term iff t is a $\bigcirc$-term.*
(2) *s is a $\circledcirc\bigcirc$-term iff t is a $\circledcirc\bigcirc$-term.*

Proof. Immediate by induction on the height of a proof tree for $P \Longrightarrow s = t$. □

Proofs of quasiequations in equational logic have a convenient graphical presentation:

Definition 37. To every set P of homogeneous identities we associate the infinite undirected graph $G(P)$ whose nodes are all pairs (x, n) where $x \in \mathsf{Vars}$ and n is a non-negative integer, and with two types of edges for $(x, n) \neq (y, k)$:
- If $\vdash P \Longrightarrow \bigcirc^n(x) = \bigcirc^k(y)$, then there is a *strong* edge between (x, n) and (y, k).

- If $\circledcirc \bigcirc^n(x) = \circledcirc \bigcirc^k(y)$ lies in P and the quasiequation $P \Longrightarrow \bigcirc^n(x) = \bigcirc^k(y)$ is not provable in equational logic, then there is a *weak* edge between (x, n) and (y, k).

By a *strong path* in $G(P)$ we mean a path consisting of strong edges.

Proposition 38. *Let P be a set of homogeneous identities, $n, k \geq 0$ and $x, y \in \mathrm{Vars}$.*
(1) $\vdash P \Longrightarrow \bigcirc^n(x) = \bigcirc^k(y)$ *iff there exists a strong path from (x, n) to (y, k) in $G(P)$.*
(2) $\vdash P \Longrightarrow \circledcirc \bigcirc^n(x) = \circledcirc \bigcirc^k(y)$ *iff there exists a path from (x, n) to (y, k) in $G(P)$.*

Proof. (1) ($\Longrightarrow$) Suppose that $\vdash P \Longrightarrow \bigcirc^n(x) = \bigcirc^k(y)$. If $(x, n) = (y, k)$, there is a trivial path of length 0 from (x, n) to (y, k). If $(x, n) \neq (y, k)$, there is a strong edge from (x, n) to (y, k), that is, an strong path of length 1.

($\Longleftarrow$) Suppose that there exists a strong path from (x, n) to (y, k) in $G(P)$, say

$$(x, n) = (x_0, n_0),\ (x_1, n_1)\ \ldots,\ (x_l, n_l) = (y, k).$$

This means that

$$\vdash P \Longrightarrow \bigcirc^{n_i}(x_i) = \bigcirc^{n_{i+1}}(x_{i+1}) \qquad (0 \leq i < l)$$

and therefore

$$\vdash P \Longrightarrow \bigcirc^n(x) = \bigcirc^k(y)$$

via reflexivity (A.3) and transitivity (A.5).

(2) ($\Longleftarrow$) Suppose that there exists a path from (x, n) to (y, k) in $G(P)$, say

$$(x, n) = (x_0, n_0),\ (x_1, n_1)\ \ldots,\ (x_l, n_l) = (y, k).$$

Then

$$\vdash P \Longrightarrow \circledcirc \bigcirc^{n_i}(x_i) = \circledcirc \bigcirc^{n_{i+1}}(x_{i+1}) \qquad (0 \leq i < l). \tag{A.11}$$

Indeed, for each i, if there is a strong edge from (x_i, n_i) to (x_{i+1}, n_{i+1}), then

$$\vdash P \Longrightarrow \bigcirc^{n_i}(x_i) = \bigcirc^{n_{i+1}}(x_{i+1})$$

and therefore

$$\vdash P \Longrightarrow \circledcirc \bigcirc^{n_i}(x_i) = \circledcirc \bigcirc^{n_{i+1}}(x_{i+1})$$

by congruence (A.6). If there is a weak edge from (x_i, n_i) to (x_{i+1}, n_{i+1}), then the identity $\bigcirc^{n_i}(x_i) = \bigcirc^{n_{i+1}}(x_{i+1})$ lies in P and therefore trivially

$$\vdash P \Longrightarrow \bigcirc^{n_i}(x_i) = \bigcirc^{n_{i+1}}(x_{i+1}).$$

From (A.11) we now get

$$\vdash P \Longrightarrow \circledcirc \bigcirc^n(x) = \circledcirc \bigcirc^k(y)$$

via reflexivity (A.3) and transitivity (A.5).

($\Longrightarrow$) Suppose that

$$\vdash P \Longrightarrow \circledcirc \bigcirc^n(x) = \circledcirc \bigcirc^k(y). \tag{A.12}$$

We prove that there exists a path from (x, n) to (y, k) in $G(P)$. The proof is by induction of the height of a proof tree for (A.12). For a proof of height 0, the identity $\circledcirc \bigcirc^n(x) = \circledcirc \bigcirc^k(y)$ is either an element of P, in which case there is an edge from (x, n) to (y, k), or it is substitution instance of reflexivity (A.3), i.e. the terms $\circledcirc \bigcirc^n(x)$ and $\circledcirc \bigcirc^k(y)$ are identical and there is a path of length 0.

Now consider a proof tree of positive height. If the last step is an substitution instance of the symmetry rule (A.4), then there is a proof of

$$P \Longrightarrow \circledcirc \bigcirc^k(y) = \circledcirc \bigcirc^n(x)$$

of smaller height. By induction, there is a path from (y, k) to (x, n), hence from (x, n) to (y, k). If the last step is an instance of the transitivity rule (A.5), then there are proofs of smaller height of

$$P \Longrightarrow \circledcirc \bigcirc^n(x) = u \qquad \text{and} \qquad P \Longrightarrow u = \circledcirc \bigcirc^k(y)$$

for some term u. By Lemma 36, the term u must have the form $u = \circledcirc \bigcirc^m(v)$ for some $m \geq 0$ and $v \in \mathrm{Vars}$. By induction, there is a path from (x, n) to (v, m) and from (v, m) to (y, k), hence from (x, n) to (y, k). If the last step is an instance of the congruence rule (A.6), then there exists a proof of smaller height of

$$P \Longrightarrow \bigcirc^n(x) = \bigcirc^k(y).$$

Thus, there is a (strong) edge from (x, n) to (y, k), i.e. a path of length 1. □

Lemma 39. *Let P be a finite set of homogeneous identities and $x, y \in \mathrm{Vars}$. For all $k < l$ and $m, n \geq 0$,*

$$\vdash \bigcirc^k(x) = \bigcirc^l(x),\ \bigcirc^m(x) = \bigcirc^n(y) \Longrightarrow \bigcirc^{m'}(x) = \bigcirc^n(y)$$
$$\vdash \bigcirc^k(x) = \bigcirc^l(x),\ \bigcirc^{m'}(x) = \bigcirc^n(y) \Longrightarrow \bigcirc^m(x) = \bigcirc^n(y)$$

where

$$m' = k + ((m-k) \bmod (l-k)).$$

Proof. By definition of m', one has $m = p \cdot (l-k) + m'$ for some integer p. From this the statements are immediate. □

Lemma 40. *Let P be a finite set of homogeneous identities and $x \in \mathrm{Vars}$. If no quasiequation $P \Longrightarrow \bigcirc^k(x) = \bigcirc^l(x)$ where $k \neq l$ is provable in equational logic, then the following holds:*

(1) *There exist only finitely many pairs $k \neq l$ such that $\vdash P \Longrightarrow \circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^l(x)$.*

(2) *If moreover $y \in \mathrm{Vars}$ and $\vdash P \Longrightarrow \bigcirc^m(y) = \bigcirc^n(y)$ for some $m \neq n$, then for every fixed q there exist only finitely many k with $\vdash P \Longrightarrow \circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^q(y)$.*

Proof. Suppose that no quasiequation $P \Longrightarrow \bigcirc^k(x) = \bigcirc^l(x)$ where $k \neq l$ is not provable in equational logic.

(1) Consider the graph $G(P)$ associated to P. For every node (y, n), there exists at most one node (x, k) with a strong edge from (y, n) to (x, k). Indeed, if there exists a second such node (x, l), $k \neq l$, we have $\vdash P \Longrightarrow \bigcirc^k(x) = \bigcirc^l(x)$, a contradiction. Consider the set $C \subseteq \mathbb{N} \times \mathbb{N}$ given by

$$\begin{aligned}(n,k) \in C \iff\ & \text{there exists } y \in \mathrm{Var} \text{ such that}\\ & \text{(i) there exists a weak edge containing the node } (y,n), \text{ and}\\ & \text{(ii) there exists a strong edge (equivalently, a strong path) from } (y,n) \text{ to } (x,k).\end{aligned}$$

Since P is finite and by the above argument, the set C is finite. Pick an upper bound K such that

$$\forall (n,k) \in C.\, k \leq K.$$

Now suppose that

$$\vdash P \Longrightarrow \circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^l(x) \tag{A.13}$$

where $k \neq l$. Then there exists a path from (x, k) to (x, l) in $G(P)$ At least one of its edges is weak; otherwise, by Proposition 38, we have $\vdash P \Longrightarrow \bigcirc^k(x) = \bigcirc^l(x)$, a contradiction. Let (y, n) be the end node of the last weak edge on the path. Then the subpath from (y, n) to (x, l) is strong, and so $(n, l) \in C$, which implies $l \leq K$. By considering the reversed path from (x, l) to (x, k) instead, we see that $k \leq K$. Hence there are only finitely many pairs $k \neq l$ with (A.13)

(2) Suppose that $\vdash P \Longrightarrow \bigcirc^m(y) = \bigcirc^n(y)$ for some $m \neq n$. Then no quasiequation $P \Longrightarrow \bigcirc^i(x) = \bigcirc^j(y)$ is provable in equational logic. (Otherwise, this proof could be used to construct a proof of some $P \Longrightarrow \bigcirc^k(x) = \bigcirc^l(x)$ where $k \neq l$.) Now fix q and let $\vdash P \Longrightarrow \circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^q(y)$. Then there exists a path from (x, k) to (y, q) in $D(P)$, and by the above argument this path is not strong. Let (z, p) be the start node of the first weak edge on the path. Consider the set C and the upper bound K as above. Then $(p, k) \in C$ and so $k \leq K$, which implies that there only finitely many choices of k.

□

Lemma 41. *Let P be a finite set of homogeneous identities and $x, y \in \mathrm{Vars}$. If $x \neq y$ and no quasiequation $P \Longrightarrow \bigcirc^k(x) = \bigcirc^l(x)$ or $P \Longrightarrow \bigcirc^k(y) = \bigcirc^l(y)$ for $k \neq l$ is provable in equational logic, then the following holds:*

(1) *For all p, p', q, q', if $\vdash P \Longrightarrow \bigcirc^p(x) = \bigcirc^q(y)$ and $\vdash P \Longrightarrow \bigcirc^{p'}(x) = \bigcirc^{q'}(y)$ then $p - q = p' - q'$.*

(2) *There exist only finitely many pairs k, l such that $\vdash P \Longrightarrow \circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^l(y)$ and the quasiequation $P \Longrightarrow \bigcirc^k(x) = \bigcirc^l(y)$ is not provable in equational logic.*

Proof. Let $x \neq y$ and suppose that no quasiequation $P \Longrightarrow \bigcirc^k(x) = \bigcirc^l(x)$ or $P \Longrightarrow \bigcirc^k(y) = \bigcirc^l(y)$ where $k \neq l$ is provable in equational logic.

(1) Suppose that $\vdash P \Longrightarrow \bigcirc^p(x) = \bigcirc^q(y)$ and $\vdash P \Longrightarrow \bigcirc^{p'}(x) = \bigcirc^{q'}(y)$. If $q = q'$, it follows by symmetry and transitivity that $\vdash P \Longrightarrow \bigcirc^p(x) = \bigcirc^{p'}(x)$, and so $p = p'$ by hypothesis, i.e. $p - q = p' - q'$. Now suppose that $q \neq q'$, say $q < q'$. Then $\vdash P \Longrightarrow \bigcirc^{p+(q'-q)}(x) = \bigcirc^{q'}(x)$ by congruence and so $\vdash P \Longrightarrow \bigcirc^{p+(q'-q)}(x) = \bigcirc^{p'}(x)$ by symmetry and transitivity. This implies $p + (q' - q) = p'$ by hypothesis, i.e. $p - q = p' - q'$.

(2) Suppose that

$$\vdash P \Longrightarrow \circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^l(y) \tag{A.14}$$

and the quasiequation $P \Longrightarrow \bigcirc^k(x) = \bigcirc^l(y)$ is not provable in equational logic. Consider again the set C and the upper bound K as defined in the proof of Lemma 40. By hypothesis, there is a path from (x, k) to (y, l) in $G(P)$ but the path is not strong. Let (z, n) be the start node of

the first weak edge on the path. Then $(n,k) \in C$ and so $k \leq K$. A symmetric argument, swapping the roles of x and y, shows that also l is bounded from above by some constant L. This shows that there are only finitely many pairs k, l satisfying (A.14). □

Proposition 42. *Let P be a finite set of homogeneous identities, and let x and y be distinct variables. Then there exists a finite set B of homogeneous identities over the variables x and y such that*

$$(u = v) \in B \quad \textit{implies} \quad \vdash P \Longrightarrow u = v, \tag{A.15}$$

and moreover, for any homogeneous identity $u = v$ where $u, v \in \Delta^*\{x, y\}$,

$$\vdash P \Longrightarrow u = v \qquad \textit{iff} \qquad \vdash B \Longrightarrow u = v. \tag{A.16}$$

We call such a set B a basis *for P w.r.t. x and y.*

Proof. Let $D(P)$ be the set of all homogeneous identities $u = v$ where $u, v \in \Delta^*\{x, y\}$ and

$$\vdash P \Longrightarrow u = v.$$

For every finite subset $B \subseteq D(P)$, the implication (A.15) and the right-to-left implication of (A.16) clearly hold. We show that there is a choice of B for which also the left-to-right implication of (A.16) holds. For this purpose, we need to distinguish several cases:

Case 1: $D(P)$ contains two identities $\bigcirc^k(x) = \bigcirc^l(x)$ and $\bigcirc^m(y) = \bigcirc^n(y)$ where $k \neq l$ and $m \neq n$.

Choose two such pairs k, l and m, n, where w.l.o.g. we assume $k < l$ and $m < n$. Let $B \subseteq D(P)$ be given by

(i) all identities $\bigcirc^p(x) = \bigcirc^q(x)$ and $\circledcirc \bigcirc^p(x) = \circledcirc \bigcirc^q(x)$ in $D(P)$ where $k \leq p, q \leq l$;

(ii) all identities $\bigcirc^p(y) = \bigcirc^q(y)$ and $\circledcirc \bigcirc^p(y) = \circledcirc \bigcirc^q(y)$ in $D(P)$ where $m \leq p, q \leq n$;

(iii) all identities $\bigcirc^p(x) = \bigcirc^q(y)$ and $\circledcirc \bigcirc^p(x) = \circledcirc \bigcirc^q(y)$ in $D(P)$ where $k \leq p \leq l$ and $m \leq q \leq n$;

Clearly, B is a finite set. We claim that the left-to-right implication of (A.16) holds. Thus suppose that $\vdash P \Longrightarrow u = v$. We only consider the case that $u = v$ is of the form $\bigcirc^p(x) = \bigcirc^q(y)$, since the other cases are entirely analogous. By Lemma 39 there exists an identity $\bigcirc^{p'}(x) = \bigcirc^{q'}(y)$ in B (namely, take $p' = k + ((p-k) \bmod (l-k))$ and $q' = m + ((q-m) \bmod (n-m))$) such that

$$\vdash \bigcirc^k(x) = \bigcirc^l(x),\ \bigcirc^m(y) = \bigcirc^n(y),\ \bigcirc^{p'}(x) = \bigcirc^{q'}(y) \Longrightarrow \bigcirc^p(x) = \bigcirc^q(y).$$

Since all three identities in the premise lie in B, we conclude $\vdash B \Longrightarrow \bigcirc^p(x) = \bigcirc^q(y)$.

Case 2: $D(P)$ contains no identity $\bigcirc^k(x) = \bigcirc^l(x)$ where $k \neq l$ but contains some identity $\bigcirc^m(y) = \bigcirc^n(y)$ where $m \neq n$.

Choose such a pair m, n, and assume w.l.o.g. that $m < n$. Let $B \subseteq D(P)$ be given by

(i) all identities $\circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^l(x)$, $k \neq l$, in $D(P)$.

(ii) all identities $\circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^q(y)$ in $D(P)$ where $m \leq q \leq n$;

(iii) all identities $\circledcirc \bigcirc^p(y) = \circledcirc \bigcirc^q(y)$ and $\circledcirc \bigcirc^p(x) = \circledcirc \bigcirc^q(x)$ in $D(P)$ where $m \leq p, q \leq n$;

Then B is a finite set by Lemma 40. Moreover, $\vdash P \Longrightarrow u = v$ implies $\vdash B \Longrightarrow u = v$:

- For $u = v$ of the form $\bigcirc^k(x) = \bigcirc^l(x)$, one has $k = l$ by hypothesis, so $\vdash B \Longrightarrow u = v$ by reflexivity.
- For $u = v$ of the form $\circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^l(x)$, if $k = l$ then $\vdash B \Longrightarrow u = v$ by reflexivity, and if $k \neq l$, then the identity $u = v$ is contained in B, so $\vdash B \Longrightarrow u = v$ trivially.
- $u = v$ cannot be of the form $\bigcirc^k(x) = \bigcirc^q(y)$, for otherwise from this and $\vdash P \Longrightarrow \bigcirc^m(y) = \bigcirc^n(y)$ a non-trivial $P \Longrightarrow \bigcirc^p(x) = \bigcirc^q(x)$ is provable.
- For $u = v$ of the form $\circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^q(y)$, one can assume w.l.o.g. that $m \leq q \leq n$ by Lemma 40, and then $u = v$ lies in B, so $\vdash B \Longrightarrow u = v$.
- For $u = v$ of the form $\bigcirc^p(y) = \bigcirc^q(y)$ or $\circledcirc \bigcirc^p(y) = \circledcirc \bigcirc^q(y)$, one can assume w.l.o.g. that $m \leq p, q \leq n$ by Lemma 39, and then $u = v$ lies in B, so $\vdash B \Longrightarrow u = v$.

Case 3: $D(P)$ contains some identity $\bigcirc^k(x) = \bigcirc^l(x)$ where $k \neq l$ but no identity $\bigcirc^m(y) = \bigcirc^n(y)$ where $m \neq n$.

Symmetric to Case 2.

Case 4. $D(P)$ contains no identity $\bigcirc^k(x) = \bigcirc^l(x)$ where $k \neq l$ and no identity $\bigcirc^m(y) = \bigcirc^n(y)$ where $m \neq n$.

We call an identity $\bigcirc^k(x) = \bigcirc^m(y)$ in $D(P)$ *minimal* if there exists no identity $\bigcirc^{k'}(x) = \bigcirc^{m'}(y)$ with $k' < k$. By Lemma 40, there exists at most one minimal identity in $D(P)$.

We let $B \subseteq D(P)$ be given by

(i) all identities $\circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^l(x)$, $k \neq l$, in $D(P)$;

(ii) the minimal identity in $D(P)$, if any;

(iii) all identities $\circledcirc \bigcirc^k(x) = \circledcirc \bigcirc^m(y)$ in $D(P)$ such that $\bigcirc^k(x) = \bigcirc^m(y)$ is not contained in $D(P)$.

(iv) all identities $\circledcirc \bigcirc^m(y) = \circledcirc \bigcirc^m(y)$, $m \neq n$, in $D(P)$.

Then B is a finite set by Lemma 40 and Lemma 41. Moreover, $\vdash P \Longrightarrow u = v$ implies $\vdash B \Longrightarrow u = v$:

- For $u = v$ of the form $\bigcirc^k(x) = \bigcirc^l(x)$ or $\bigcirc^k(y) = \bigcirc^l(y)$, one has $k = l$ and so $\vdash B \Longrightarrow u = v$ by reflexivity.
- For $u = v$ of the form $\circledcirc\bigcirc^k(x) = \circledcirc\bigcirc^l(x)$ or $\circledcirc\bigcirc^k(y) = \circledcirc\bigcirc^l(y)$, the identity $u = v$ lies in B, so $\vdash B \Longrightarrow u = v$ trivially.
- For $u = v$ of the form $\bigcirc^k(x) = \bigcirc^m(y)$, the identity is provable via congruence from the minimal identity in $D(P)$ by Lemma 41, and so $\vdash B \Longrightarrow u = v$ since the latter lies in B.
- For $u = v$ of the form $\circledcirc\bigcirc^k(x) = \circledcirc\bigcirc^m(y)$, if $\bigcirc^k(x) = \bigcirc^m(y)$ in $D(P)$, then $u = v$ is provable from the minimal identity (which lies in B) via congruence; otherwise, the identity $u = v$ lies in B. In both cases, $\vdash B \Longrightarrow u = v$.

This concludes the proof of (A.16). □

Proposition 43. *Let P a finite set of homogeneous identities, and let B be a finite basis for P w.r.t. x and y. Then for any homogeneous identity $u = v$ where $u, v \in \Delta^*\{x, y\}$,*

$$P \Longrightarrow u = v \text{ is valid} \qquad \text{iff} \qquad B \Longrightarrow u = v \text{ is valid.} \tag{A.17}$$

Proof. We use the notation $D(P)$ from the proof of Proposition 42. Clearly, since $B \subseteq D(P)$, the right-to-left implication holds. Conversely, suppose that $P \Longrightarrow u = v$ is valid, let A be a set, and let $\mathfrak{I}\colon \mathrm{Vars} \to A^\omega$ be a variable interpretation such that

$$^{\mathfrak{I}}[\![s]\!] = {}^{\mathfrak{I}}[\![t]\!] \quad \text{for all } s = t \text{ in B.} \tag{A.18}$$

It suffices show that there exists an interpretation $\overline{\mathfrak{I}}\colon \mathrm{Vars} \to A^\omega$ such that

$$\overline{\mathfrak{I}}(x) = \mathfrak{I}(x), \quad \overline{\mathfrak{I}}(y) = \mathfrak{I}(y), \quad {}^{\overline{\mathfrak{I}}}[\![s]\!] = {}^{\overline{\mathfrak{I}}}[\![t]\!] \quad \text{for all } s = t \text{ in P.} \tag{A.19}$$

Then, since $P \Longrightarrow u = v$ is valid and $u, v \in \Delta^*\{x, y\}$, it follows that

$$^{\mathfrak{I}}[\![u]\!] = {}^{\overline{\mathfrak{I}}}[\![u]\!] = {}^{\overline{\mathfrak{I}}}[\![v]\!] = {}^{\mathfrak{I}}[\![v]\!]$$

proving that $B \Longrightarrow u = v$ is valid. For the definition of $\overline{\mathfrak{I}}$, we consider the graph $G(P)$ (Definition 37). For each connected component $C \subseteq \mathrm{Vars} \times \mathbb{N}$, we define an element $a_C \in A$ as follows:

- If C contains a node $(z, n) \in C$ where $z \in \{x, y\}$, put
$$a_C := \mathfrak{I}(z)(n).$$
Note that a_C is independent of the choice of (z, n): if (w, m) is another element of C where $w \in \{x, y\}$, then there exists a path from (z, n) to (w, m) in $G(P)$, so
$$\vdash P \Longrightarrow \circledcirc\bigcirc^n(z) = \circledcirc\bigcirc^m(w).$$
This implies
$$\vdash B \Longrightarrow \circledcirc\bigcirc^n(z) = \circledcirc\bigcirc^m(w)$$
by (A.16), in particular the quasiequation $B \Longrightarrow \circledcirc\bigcirc^n(z) = \circledcirc\bigcirc^m(w)$ is valid. Therefore, from (A.18) it follows that $^{\mathfrak{I}}[\![\circledcirc\bigcirc^n(z)]\!] = {}^{\mathfrak{I}}[\![\circledcirc\bigcirc^k(w)]\!]$, which means
$$\mathfrak{I}(z)(n) = \mathfrak{I}(w)(k).$$
- If C does not contain any node (z, n) where $z \in \{x, y\}$, choose an arbitrary element $a_C \in A$.

Now define $\overline{\mathfrak{I}}\colon \mathrm{Vars} \to A^\omega$ by

$$\overline{\mathfrak{I}}(z)(n) = a_{C_{(z,n)}} \qquad \text{where } C_{(z,n)} \text{ is the connected component of } (z, n) \text{ in } G(P).$$

We show that $\overline{\mathfrak{I}}$ satisfies the desired properties (A.19). Indeed, if $z \in \{x, y\}$, then

$$\overline{\mathfrak{I}}(z)(n) = a_{C_{(z,n)}} = \mathfrak{I}(z)(n) \qquad \text{for all } n \geq 0$$

by definition of $a_{C_{(z,n)}}$, and so $\mathfrak{I}(z) = \overline{\mathfrak{I}}(z)$. Now suppose that $s = t$ is an identity in P. If $s = t$ is a $\bigcirc$-identity $\bigcirc^k(z) = \bigcirc^l(w)$ then for every $n \in \mathbb{N}$ the pairs $(z, k + n)$ and $(w, l + n)$ lie in the same connected component of $G(P)$ since they are connected by a strong edge, and so

$$^{\overline{\mathfrak{I}}}[\![s]\!](n) = {}^{\overline{\mathfrak{I}}}[\![\bigcirc^k(z)]\!](n) = \overline{\mathfrak{I}}(z)(k + n) = a_{C_{(z,k+n)}} = a_{C_{(w,l+n)}} = \overline{\mathfrak{I}}(w)(l + n) = {}^{\overline{\mathfrak{I}}}[\![\bigcirc^l(w)]\!](n) = {}^{\overline{\mathfrak{I}}}[\![t]\!](n),$$

whence $^{\overline{\mathfrak{I}}}[\![s]\!] = {}^{\overline{\mathfrak{I}}}[\![t]\!]$. Similarly, if $s = t$ is a $\circledcirc\bigcirc$-identity $\circledcirc\bigcirc^k(z) = \circledcirc\bigcirc^l(w)$, then the pairs (z, k) and (w, l) lie in the same connected component of $G(P)$ since they are connected by a (strong or weak) edge, whence

$$^{\overline{\mathfrak{I}}}[\![s]\!] = {}^{\overline{\mathfrak{I}}}[\![\circledcirc\bigcirc^k(z)]\!] = (\overline{\mathfrak{I}}(z)(k))^\omega = (a_{C_{(z,k)}})^\omega = (a_{C_{(w,l)}})^\omega = (\overline{\mathfrak{I}}(w)(l))^\omega = {}^{\overline{\mathfrak{I}}}[\![\bigcirc^l(w)]\!] = {}^{\overline{\mathfrak{I}}}[\![t]\!].$$

This concludes the proof. □

The existence of finite bases allows us to reduce quasiequations to a very simple form:

Definition 44. Fix a pair of distinct variables $x \neq y$. A quasiequation $P \Longrightarrow s = t$ is *normalized (w.r.t. x and y)* if the following conditions hold:

(N1) All identities in P are homogeneous.

(N2) The term s and t and all terms occurring in P are elements of $\Delta^*\{x, y\}$.

(N3) P contains no identity of the form $\bigcirc^l(y) = \bigcirc^k(x)$.

(N4) All identities in P of the form $\bigcirc^k(x) = \bigcirc^l(y)$ have the same degree k on the left hand side.

(N5) If the identities $\bigcirc^k(x) = \bigcirc^l(y)$ and $\bigcirc^k(x) = \bigcirc^m(y)$ lie in P, then so does $\bigcirc^l(y) = \bigcirc^m(y)$.

Definition 45. Given a set Ax of quasiequations, a set Ax′ of quasiequations *strengthens* Ax if every quasiequation in Ax is Ax′-provable (equivalently, by Remark 30, if every Ax-provable quasiequation is Ax′-provable).

Theorem 46 (Normalization). *For every finite set* Ax *of valid quasiequations, there exists a finite set* Ax′ *of valid quasiequations such that* Ax′ *strengthens* Ax *and all quasiequations contained in* Ax′ *except* (A.7)–(A.10) *are normalized.*

Proof. We may assume that Ax contains the quasiequations (A.7)–(A.10), which are all valid; otherwise, add them to Ax. We show how to replace, step by step, non-normalized quasiequations in Ax (i.e. quasiequations *not* satisfying one of the requirements (N1)–(N5)) with equivalent normalized ones, until a set of valid quasiequations is reached that strenghtens Ax and contains, except for (A.7)–(A.10), only normalized quasiequations.

(N1) Suppose that Ax contains, except from (A.7)–(A.10), some quasiequation of the form

$$P,\ \bigcirc^k(z) = u \Longrightarrow s = t \tag{A.20}$$

where u contains $\circledcirc$. (The case $u = \bigcirc^k(z)$ is handled symmetrically.) Thus $u = v(\circledcirc \bigcirc^m(w))$ for some unique term v and variable w. Replace (A.20) with

$$P,\ \bigcirc^{k+1}(z) = \bigcirc^k(z),\ \circledcirc \bigcirc^k(z) = \circledcirc \bigcirc^m(w) \Longrightarrow s = t. \tag{A.21}$$

This quasiequation is valid since the identity $\bigcirc^k(z) = v(\circledcirc \bigcirc^m(w))$ is semantically equivalent to the conjunction of $\bigcirc^{k+1}(z) = \bigcirc^k(z)$ and $\circledcirc \bigcirc^k(z) = \circledcirc \bigcirc^m(w)$. Moreover, the quasiequation (A.20) is provable from (A.21) using equational logic and (A.7)–(A.10). Therefore, the resulting set of axioms strengthens Ax (Remark 30). Repeating this process yields a strengthening of Ax where all quasiequations except (A.7)–(A.10) satisfy (N1).

(N2) Suppose that all quasiequations in Ax except (A.7)–(A.10) satisfy (N1). First, by renaming variables if necessary, we may assume that for every $P \Longrightarrow s = t$ in Ax, one has $s, t \in \Delta^*\{x, y\}$. Replace every quasiequation

$$P \Longrightarrow s = t \tag{A.22}$$

in Ax not satisfying (N2), that is, with variables distinct from x, y in the premise, by the quasiequation

$$B \Longrightarrow s = t \tag{A.23}$$

where B is a finite basis of P w.r.t. x and y (Proposition 42). Then (A.23) is valid by Proposition 43. Moreover, since $\vdash P \Longrightarrow u = v$ for all $u = v$ in B by (A.15), the quasiequation (A.22) is provable from (A.23). Thus we obtain a strengthening of Ax where all quasiequations except (A.7)–(A.10) satisfy (N1) and (N2).

(N3) Suppose that all quasiequations in Ax except (A.7)–(A.10) satisfy (N1) and (N2), and that Ax contains a quasiequation

$$P,\ \bigcirc^l(y) = \bigcirc^k(x) \Longrightarrow s = t. \tag{A.24}$$

Then replace this quasiequation with

$$P,\ \bigcirc^k(x) = \bigcirc^l(y) \Longrightarrow s = t. \tag{A.25}$$

This quasiequation is valid because $\bigcirc^l(y) = \bigcirc^k(x)$ and $\bigcirc^k(x) = \bigcirc^l(y)$ are semantically equivalent. Moreover, (A.24) is provable from (A.25) via symmetry (A.4), so the resulting set of axioms strengthens Ax. By repeating this process, we end up with a strengthening of Ax where all quasiequations except (A.7)–(A.10) satisfy (N1)–(N3).

(N4) Suppose that all axioms in Ax except (A.7)–(A.10) satisfy (N1)–(N3), and that Ax contains a quasiequation

$$P, \bigcirc^k(x) = u, \bigcirc^l(x) = v \Longrightarrow s = t \tag{A.26}$$

where u and v are $\bigcirc$-terms over $\{y\}$ and $k \neq l$, say $k < l$. Replace (A.26) with

$$P, \bigcirc^l(x) = \bigcirc^{l-k}u,\ \circledcirc \bigcirc^{k+i}(x) = \circledcirc \bigcirc^i(u)\ (i = 0, \ldots, l-k),\ \bigcirc^l(x) = v \Longrightarrow s = t. \tag{A.27}$$

This quasiequation is valid because $\bigcirc^k(x) = u$ is semantically equivalent to the conjunction of the identities $\bigcirc^l(x) = \bigcirc^{l-k}u$ and $\circledcirc \bigcirc^{k+i}(x) = \circledcirc \bigcirc^i(u)$ for $i = 0, \ldots, l-k$. Moreover (A.26) is provable from (A.27) using the congruence rule (A.6) of equational logic. Thus the resulting set of axioms strengthens Ax. By repeating this process, we obtain a strengthening of Ax where all quasiequations except (A.7)–(A.10) satisfy (N1)–(N4).

(N5) Finally, suppose that all axioms in Ax except (A.7)–(A.10) satisfy (N1)–(N4), and that Ax contains a quasiequation

$$P, \bigcirc^k(x) = \bigcirc^l(y),\ \bigcirc^k(x) = \bigcirc^m(y) \Longrightarrow s = t \tag{A.28}$$

where $l \neq m$ and $\bigcirc^l(y) = \bigcirc^m(y)$ does not appear in P. Replace (A.28) with

$$P, \bigcirc^k(x) = \bigcirc^l(y),\ \bigcirc^k(x) = \bigcirc^m(y),\ \bigcirc^l(y) = \bigcirc^m(y) \Longrightarrow s = t. \tag{A.29}$$

This quasiequation is valid because the conjunction of $\bigcirc^k(x) = \bigcirc^l(y)$ and $\bigcirc^k(x) = \bigcirc^m(y)$ is semantically equivalent to the conjunction of $\bigcirc^k(x) = \bigcirc^l(y)$, $\bigcirc^k(x) = \bigcirc^m(y)$, and $\bigcirc^l(y) = \bigcirc^m(y)$. Moreover, (A.28) is provable from (A.29) using the symmetry (A.4) and transitivity rules (A.5) of equational logic. Thus the resulting set of axioms strengthens Ax. Repeating this process yields a strengthening of Ax where all quasiequations except (A.7)–(A.10) satisfy (N1)–(N5), and thus are normalized. □

A.12.3 Finite Axiomatizability. We are now ready to prove the non-existence of finite axiomatizations for the quasiequational theory of discrete stream algebras. A discrete axiom system Ax (i.e. a set of finitary Δ-quasiequations) is *sound* for discrete sequence algebras if every quasiequation from Ax is valid for discrete sequence algebras, or equivalently, if every quasiequation provable from Ax is valid for discrete sequence algebras. The axiom system Ax is *complete* for discrete sequence algebras if every quasiequation that is valid for discrete sequence algebras has a finite derivation from Ax.

Theorem 18 (Incompleteness). *There is no finite discrete axiom system that is both sound and complete for discrete sequence algebras.*

Proof. Suppose towards a contradiction that there exists a finite discrete axiom system Ax that is sound and complete for discrete sequence algebras. By Theorem 46, we may assume w.l.o.g. that all quasiequations in Ax except (A.7)–(A.10) are normalized w.r.t. the variables x and y. The key to the proof is to exploit that, since Ax is finite and all quasiequations in Ax are finitary, for $\bigcirc$-identities $\bigcirc^k(z) = \bigcirc^l(z)$, $z \in \{x, y\}$, arising in the premise of any quasiequation in Ax, the difference $|k - l|$ of the degrees of the $\bigcirc$-terms is necessarily bounded from above. In other words, we can choose a natural number N such that

$$(P \Longrightarrow s = t) \in \mathsf{Ax} \quad \text{and} \quad (\bigcirc^k(z) = \bigcirc^l(z)) \in P \qquad \text{implies} \qquad |k - l| < N. \tag{A.30}$$

Fix a variable $a \in \mathsf{Vars}$ and consider the following quasiequations:

$$\bigcirc^N(a) = a,\ \circledcirc\bigcirc^k(a) = \circledcirc\bigcirc^{k+1}(a)\ (0 \le k < N) \Longrightarrow \bigcirc^i(a) = \bigcirc^j(a) \qquad (N \nmid i - j) \tag{A.31}$$

$$\bigcirc^N(a) = a,\ \circledcirc\bigcirc^k(a) = \circledcirc\bigcirc^{k+1}(a)\ (0 \le k < N) \Longrightarrow s = t \tag{A.32}$$

where $i, j \ge 0$, and s, t ranges over all pairs of terms in $\Delta^*\{a\}$ such that one of the two terms is a $\bigcirc$-term and the other contains $\circledcirc$. Note that all the above quasiequations have the same premise $\overline{P}$. Moreover, they are all valid for discrete sequence algebras since the premise $\overline{P}$ semantically implies that a represents a flat sequence. Therefore, by completeness of Ax, each of the quasiequations (A.31) and (A.32) is Ax-provable. Among them, choose a quasiequation

$$\overline{P} \Longrightarrow s_{\min} = t_{\min} \tag{A.33}$$

with a proof from Ax of minimum height $h_{\min}$. Fix a proof tree of (A.33) of height $h_{\min}$, and let

$$P \Longrightarrow s = t \tag{A.34}$$

be the axiom from $\mathsf{Ax} \cup \mathsf{Ax}_=$ used in the last proof step. We now consider several cases, corresponding to the type of axiom used, and demonstrate that in each case a contradiction arises.

Case 1: (A.34) is the reflexivity axiom (A.3) from $\mathsf{Ax}_=$.

Then $s_{\min}$ and $t_{\min}$ are identical terms, but this not the case for the conclusion of any of the quasiequations (A.31) and (A.32), a contradiction.

Case 2: (A.34) is the symmetry axiom (A.4) from $\mathsf{Ax}_=$.

Then there exists a proof of $\overline{P} \Longrightarrow t_{\min} = s_{\min}$ from Ax of height $h_{\min} - 1$. This is a quasiequation of the form (A.31) or (A.32), since (A.33) is, contradicting the minimal choice of (A.33).

Case 3: (A.34) is the transitivity axiom (A.4) from $\mathsf{Ax}_=$. Then there exists a term u such that

$$\overline{P} \Longrightarrow s_{\min} = u \qquad \text{and} \qquad \overline{P} \Longrightarrow u = t_{\min} \tag{A.35}$$

have a proof from Ax of height less than $h_{\min}$. By definition of (A.31) and (A.32), one of the terms $s_{\min}$ or $t_{\min}$ is a $\bigcirc$-term, say $s_{\min} = \bigcirc^k(a)$ (the other case is symmetric). Note that u must be a term in the variable a: otherwise, since the premise $\overline{P}$ contains only terms in a, the Ax-provable quasiequation $\overline{P} \Longrightarrow s_{\min} = u$ is clearly not valid, contradicting soundness of Ax. We consider two subcases:

Subcase 3.1: u contains $\circledcirc$.

Then $\overline{P} \Longrightarrow s_{\min} = u$ is one of the quasiequations (A.32), and it has a proof of height less than $h_{\min}$, which is impossible.

Subcase 3.2: $u = \bigcirc^l(a)$ for some $l \ge 0$.

Then the Ax-provable quasiequations (A.35) take the form

$$\overline{P} \Longrightarrow \bigcirc^k(a) = \bigcirc^l(a) \qquad \text{and} \qquad \overline{P} \Longrightarrow \bigcirc^l(a) = t_{\min}.$$

Then $t_{\min}$ cannot contain $\circledcirc$, since otherwise the second quasiequation above is of type (A.32) and has a proof tree of height less than $h_{\min}$, which is impossible. Thus $t_{\min} = \bigcirc^m(a)$ for some $m \ge 0$. Since the above two quasiequations have proof trees of height less than $h_{\min}$, they cannot be of the form (A.31), so N divides both $k - l$ and $l - m$. Thus N divides $k - m$. But this is impossible: since (A.33) is the quasiequation

$$\overline{P} \Longrightarrow \bigcirc^k(a) = \bigcirc^m(a)$$

and thus of the form (A.31), we have that N does not divide $k - m$.

Case 4: (A.34) is the congruence axiom (A.6) from $\mathsf{Ax}_=$.

Then there exists a quasiequation

$$\overline{P} \Longrightarrow u = v \tag{A.36}$$

with a proof of height $h_{\min} - 1$ such that $\mathsf{f}(u) = s_{\min}$ and $\mathsf{f}(v) = t_{\min}$ for some $\mathsf{f} \in \{\circledcirc, \bigcirc\}$. Since $s_{\min}$ or $t_{\min}$ is a $\bigcirc$-term (say $s_{\min}$), we have $\mathsf{f} = \bigcirc$, and moreover u is a $\bigcirc$-term. If the term v contains $\circledcirc$, then (A.36) is a quasiequation of type (A.32), which is impossible because it has a proof of height less than $h_{\min}$. If v is a $\bigcirc$-term, then (A.36) takes the form

$$\overline{P} \Longrightarrow \bigcirc^i(a) = \bigcirc^j(a)$$

for some $i, j \geq 0$, and $s_{\min} = \bigcirc^{i+1}(a)$ and $t_{\min} = \bigcirc^{j+1}(a)$. Since $i - j = (i+1) - (j+1)$, the quasiequation (A.36) is of type (A.31). This is impossible since it has a proof of height less than $h_{\min}$.

Case 5: (A.34) is the one of the quasiequations (A.7)–(A.10).

We first note that no substitution instance of the conclusion of (A.7)–(A.9) is a $\bigcirc$-identity or an equation where one term is a $\bigcirc$-term and the other contains $\circledcirc$. Therefore, neither of these quasiequations can be used in the last step of a proof of (A.33). It thus only remains to consider the case where (A.34) is (A.10), i.e.

$$x = \circledcirc(y) \Longrightarrow \bigcirc(x) = x.$$

Then there exists a substitution σ such that

$$s_{\min} = \bigcirc(\sigma(x)) \qquad \text{and} \qquad t_{\min} = \sigma(x).$$

Then $\sigma(x)$ is necessarily a $\bigcirc$-term in $\Delta^*\{a\}$ (otherwise (A.33) cannot be of the form (A.31) or (A.32)). Therefore, we have a proof of

$$\overline{P} \Longrightarrow \sigma(x) = \circledcirc(\sigma(y)) \tag{A.37}$$

from Ax of height $h_{\min} - 1$, where $\sigma(x)$ is a $\bigcirc$-term in $\Delta^*\{a\}$ and $\circledcirc(\sigma(y))$ contains $\circledcirc$. Note that $\sigma(y) \in \Delta^*\{a\}$, for otherwise the quasiequation (A.37) is not valid, contradicting soundness of Ax. Therefore, (A.37) is a quasiequation of type (A.32), contradicting the minimal choice of (A.33).

Case 6: (A.34) is a quasiequation from Ax and none of (A.7)–(A.10).

Then (A.34) is normalized, i.e. satisfies (N1)–(N5) of Definition 44. Moreover, there exists a substitution σ such that

$$s_{\min} = s[\sigma] \qquad \text{and} \qquad t_{\min} = t[\sigma], \tag{A.38}$$

and

$$\mathsf{Ax} \vdash \overline{P} \Longrightarrow u[\sigma] = v[\sigma] \qquad \text{for all } (u = v) \in P \tag{A.39}$$

with respective proofs from Ax of height less than $h_{\min}$. We start with a simple observation; in the following, we write $\bigcirc^*$ for $\bigcirc^p$ if the specific exponent p does not matter .

($\star$) *Claim.* If $z \in \{x, y\}$ and $\sigma(z) = \bigcirc^*(a)$, then P contains no identity $\bigcirc^k(z) = \bigcirc^l(z)$ where $k \neq l$.

Proof. Suppose that P contains some identity $\bigcirc^k(z) = \bigcirc^l(z)$ where $k, l \geq 0$, and let $\sigma(z) = \bigcirc^j(a)$. Then, by (A.39) we have that $\mathsf{Ax} \vdash \overline{P} \Longrightarrow \bigcirc^{k+j}(a) = \bigcirc^{l+j}(a)$ with a proof of height less than $h_{\min}$. This means that this quasiequation is not of type (A.31), so N divides $(k + j) - (l + j) = k - l$. On the other hand, we have $|k - l| < N$ by the choice (A.30) of the upper bound N, and so necessarily $k - l = 0$, i.e. $k = l$. This proves ($\star$).

Since (A.33) is a quasiequation of type (A.31) or (A.32), at least one of the terms $s_{\min}$ or $t_{\min}$ is a $\bigcirc$-term; by symmetry, we assume that $s_{\min}$ is a $\bigcirc$-term. Since $s_{\min} = s[\sigma]$, also s is a $\bigcirc$-term:

$$s = \bigcirc^i(z) \qquad \text{for some } i \geq 0 \text{ and } z \in \{x, y\}. \tag{A.40}$$

Moreover, we have

$$\sigma(z) = \bigcirc^j(a) \qquad \text{for some } j \geq 0$$

so that

$$s_{\min} = \bigcirc^{i+j}(a).$$

Choose an upper bound to the degrees of $\circledcirc\bigcirc$-identities in P, that is, a natural number K such that, for all $v, w \in \{x, y\}$,

$$(\circledcirc\bigcirc^k(v) = \circledcirc\bigcirc^l(w)) \in P \qquad \text{implies} \qquad k, l \leq K. \tag{A.41}$$

We now consider several subcases, corresponding to whether the variable $z \in \{x, y\}$ of (A.40) is x or y, and to which kinds of identities occur in P.

Subcase 6.1: $z = x$, and P contains some identity $\bigcirc^k(x) = \bigcirc^m(y)$ where $k, m \geq 0$.

Let us make the following observations:

(O1) P contains no non-trivial identity $\bigcirc^*(x) = \bigcirc^*(x)$. This follows from ($\star$) since $\sigma(x) = \bigcirc^*(a)$.

(O2) We have $\sigma(y) = \bigcirc^*(a)$. Indeed, $\sigma(y)$ cannot contain a variable $b \neq a$, since otherwise the quasiequation $\overline{P} \Longrightarrow \bigcirc^k(\sigma(x)) = \bigcirc^m(\sigma(y))$, which is Ax-provable by (A.39), is clearly not valid, contradicting the soundness of Ax. Moreover, it is not possible that $\sigma(y) = u$ for a term u using $\circledcirc$, since then we have a proof of $\overline{P} \Longrightarrow \bigcirc^k(\sigma(x)) = \bigcirc^m(\sigma(y))$ of height less than $h_{\min}$ and this quasiequation is of type (A.32), a contradiction.

(O3) P contains no non-trivial identity $\bigcirc^*(y) = \bigcirc^*(y)$. This follows from (O2) and ($\star$).

(O4) The identity $\bigcirc^k(x) = \bigcirc^m(y)$ is the unique identity of type $\bigcirc^*(x) = \bigcirc^*(y)$ in P. Indeed, suppose that there is another such identity $\bigcirc^l(x) = \bigcirc^n(y)$ where $(k,m) \neq (l,n)$. By the normalization condition (N4) we know that $k = l$. Therefore $m \neq n$, and by (N5) the identity $\bigcirc^m(y) = \bigcirc^n(y)$ lies in P, contradicting (O3).

In summary, we have shown that P contains only one non-trivial $\bigcirc$-identity, namely $\bigcirc^k(x) = \bigcirc^m(y)$. Fix a countably infinite set

$$A = \{\bot, a_1, a_2, a_3, \ldots\} \tag{A.42}$$

and define the interpretation $\mathfrak{I}\colon \{x,y\} \to A^\omega$ by

$$\mathfrak{I}(x) = \bot^{K+k} a_1 a_2 a_3 \cdots \qquad \text{and} \qquad \mathfrak{I}(y) = \bot^{K+m} a_1 a_2 a_3 \cdots \tag{A.43}$$

where K is the upper bound on the degrees of $\circledcirc\bigcirc$-identities in P given by (A.41). Then all identities in P are satisfied under $\mathfrak{I}$: for the identity $\bigcirc^k(x) = \bigcirc^m(y)$ this is clear, and all $\circledcirc\bigcirc$-identities in P are satisfied because they refer to the first K elements of $\mathfrak{I}(x)$ and $\mathfrak{I}(y)$, which have value $\bot$.

We now look at the conclusion of the axiom (A.34), recalling that $s = \bigcirc^i(x)$:

Subsubcase 6.1.1: (A.34) is of the form $P \Longrightarrow \bigcirc^i(x) = \bigcirc^p(x)$ where $p \geq 0$.

Then (A.33) is the quasiequation $\overline{P} \Longrightarrow \bigcirc^i(\sigma(x)) = \bigcirc^p(\sigma(x))$, i.e. $\overline{P} \Longrightarrow \bigcirc^{i+j}(a) = \bigcirc^{p+j}(a)$ since $\sigma(x) = \bigcirc^j(a)$. Thus it is a quasiequation of type (A.31), and so N does not divide $(i+j)-(p+j) = i-p$. On the other hand, since all identities in P are satisfied under $\mathfrak{I}$ and the axiom (A.34) is valid, it follows that $\bigcirc^i(\mathfrak{I}(x)) = \bigcirc^p(\mathfrak{I}(x))$. But by definition of $\mathfrak{I}(x)$, this is only possible if $i = p$. In particular N divides $i - p$, a contradiction.

Subsubcase 6.1.2: (A.34) is of the form $P \Longrightarrow \bigcirc^i(x) = \bigcirc^p(y)$ where $p \geq 0$.

Since all identities in P are satisfied under $\mathfrak{I}$ and the axiom (A.34) is valid, it follows that $\bigcirc^i(\mathfrak{I}(x)) = \bigcirc^p(\mathfrak{I}(y))$. By definition of $\mathfrak{I}(x)$ and $\mathfrak{I}(y)$, this is only possible if

$$k - m = i - p.$$

Now consider the quasiequation (A.33), i.e. $\overline{P} \Longrightarrow \bigcirc^i(\sigma(x)) = \bigcirc^p(\sigma(y))$. We have $\sigma(x) = \bigcirc^j(a)$ and $\sigma(y) = \bigcirc^q(a)$ for some $q \geq 0$, the latter by (O2). Thus (A.33) is of the form (A.31), which means that N does not divide $(i+j)-(p+q)$. Now by (A.39) the quasiequation $\overline{P} \Longrightarrow \bigcirc^k(\sigma(x)) = \bigcirc^m(\sigma(y))$ has a proof from Ax of height less than $h_{\min}$. This quasiequation is equal to

$$\overline{P} \Longrightarrow \bigcirc^{k+j}(a) = \bigcirc^{m+q}(a), \tag{A.44}$$

and we have

$$(k+j)-(m+q) = (k-m)+(j-q) = (i-p)+(j-q) = (i+j)-(p+q).$$

Thus N also does not divide $(k+j)-(m+q)$, which means that (A.44) is a quasiequation of type (A.31) with a proof of height less than $h_{\min}$, a contradiction.

Subsubcase 6.1.3: (A.34) is of the form $P \Longrightarrow \bigcirc^i(x) = t$ where t contains $\circledcirc$.

Since all identities in P are satisfied under $\mathfrak{I}$ and (A.34) is valid, it follows that $\bigcirc^i(\mathfrak{I}(x)) = {}^{\mathfrak{I}}[\![t]\!]$. But this is impossible: the sequence ${}^{\mathfrak{I}}[\![t]\!]$ is flat (since t contains $\circledcirc$) but the sequence $\bigcirc^i(\mathfrak{I}(x))$ is not.

Subcase 6.2: $z = y$, and P contains some identity $\bigcirc^k(x) = \bigcirc^m(y)$ where $k, m \geq 0$.

Using arguments symmetric to Subcase 6.1, one shows that

(O1') P contains no non-trivial identity $\bigcirc^*(y) = \bigcirc^*(y)$.

(O2') $\sigma(x) = \bigcirc^*(a)$.

(O3') P contains no non-trivial identity $\bigcirc^*(x) = \bigcirc^*(x)$.

(O4') The identity $\bigcirc^k(x) = \bigcirc^m(y)$ is the unique identity of type $\bigcirc^*(x) = \bigcirc^*(y)$ in P.

Therefore P contains only one non-trivial $\bigcirc$-identity. The rest of the argument is exactly like in Subcase 6.1.

Subcase 6.3: $z = x$, and P contains no identity $\bigcirc^k(x) = \bigcirc^m(y)$ where $k, m \geq 0$.

We first observe that

(O1") P contains no non-trivial identity $\bigcirc^*(x) = \bigcirc^*(x)$. This follows from ($\star$) since $\sigma(x) = \bigcirc^j(a)$.

Take the set A given by (A.42) and define the interpretation $\overline{\mathfrak{I}}\colon \{x, y\} \to A^\omega$ by

$$\overline{\mathfrak{I}}(x) = \bot^K a_1 a_2 a_3 \cdots \qquad \text{and} \qquad \overline{\mathfrak{I}}(y) = \bot^\omega \tag{A.45}$$

Then all identities in P are satisfied under $\overline{\mathfrak{I}}$: all $\circledcirc\,\bigcirc$-identities are satisfied because they refer only to the first K elements of $\overline{\mathfrak{I}}(x)$ and $\overline{\mathfrak{I}}(y)$ by (A.41), and all non-trivial $\bigcirc$-identities are of the form $\bigcirc^*(y) = \bigcirc^*(y)$, and they are satisfied because $\overline{\mathfrak{I}}(y)$ is a flat sequence.

We now consider the axiom (A.34) and distinguish three cases:

Subsubcase 6.3.1: (A.34) is of the form $P \Longrightarrow \bigcirc^i(x) = \bigcirc^p(x)$ where $p \geq 0$.

Then (A.33) is the quasiequation $\overline{P} \Longrightarrow \bigcirc^i(\sigma(x)) = \bigcirc^p(\sigma(x))$, i.e. $\overline{P} \Longrightarrow \bigcirc^{i+j}(a) = \bigcirc^{p+j}(a)$ since $\sigma(x) = \bigcirc^j(a)$. Thus it is a quasiequation of type (A.31), and so N does not divide $(i + j) - (p + j) = i - p$. On the other hand, since (A.34) is valid and all identities in P are satisfied under the interpretation $\overline{\mathfrak{I}}$, it follows that $\bigcirc^i(\overline{\mathfrak{I}}(x)) = \bigcirc^p(\overline{\mathfrak{I}}(x))$. But by definition of $\overline{\mathfrak{I}}(x)$, this is only possible if $i = p$. In particular N divides $i - p$, a contradiction.

Subsubcase 6.3.2: (A.34) is of the form $P \Longrightarrow \bigcirc^i(x) = \bigcirc^p(y)$ where $p \geq 0$.

Since (A.34) is valid and all identities in P are satisfied under the interpretation $\overline{\mathfrak{I}}$, it follows that $\bigcirc^i(\overline{\mathfrak{I}}(x)) = \bigcirc^p(\overline{\mathfrak{I}}(y))$. But this is impossible because $\bigcirc^p(\overline{\mathfrak{I}}(y))$ is flat and $\bigcirc^i(\overline{\mathfrak{I}}(x))$ is not.

Subsubcase 6.3.3: (A.34) is of the form $P \Longrightarrow \bigcirc^i(x) = t$ where t contains $\circledcirc$.

Since (A.34) is valid and all identities in P are satisfied under the interpretation $\overline{\mathfrak{I}}$, it follows that $\bigcirc^i(\overline{\mathfrak{I}}(x)) = {}^{\overline{\mathfrak{I}}}[\![t]\!]$. But this is impossible: the sequence ${}^{\overline{\mathfrak{I}}}[\![t]\!]$ is flat (since t contains $\circledcirc$) but $\bigcirc^i(\overline{\mathfrak{I}}(x))$ is not.

Subcase 6.4: $z = y$, and P contains no identity $\bigcirc^k(x) = \bigcirc^m(y)$ where $k, m \geq 0$.

Analogous to Subcase 6.3.

This concludes the proof of Theorem 18. □

A.13 Appendix to Section 6.2

Let us begin our approach towards the completeness proof for AIC_ω.

Completeness of infinitary quasiequational logic

As stated, it appears that the completeness of well-founded derivations for infinitary Horn logic is folklore. We include a proof here for convenience's sake, although we make no claim for originality.

Theorem 20 (Soundness and Completeness of Well-founded Derivations). *Let* Ax *be an axiom system and let* Q *be a quasiequation. Then* $\mathsf{Ax} \vdash_{\mathsf{wf}} \mathsf{Q}$ *if and only if for any AIC-structure* $\mathcal{A} \models \mathsf{Ax}$*, we also have* $\mathcal{A} \models \mathsf{Q}$.

Proof. We are only going to cover the case where I is always a countable set, since this is the case relevant to AIC_ω. However, our proof extends to the general case by replacing ω_1 with another regular cardinal that is an upper bound on the cardinalities of the index sets I that appear in quasiequations in Ax.

($\Rightarrow$) Let us begin with *soundness*. Suppose that $\mathsf{Q} = (\bigwedge_{i\in I} {}^i s = {}^i t) \Longrightarrow s = t$ is a quasiequation such that $\mathsf{Ax} \vdash_{\mathsf{wf}} \mathsf{Q}$, and that $\mathcal{A}$ is an AIC-structure with $\mathcal{A} \models \mathsf{Ax}$. We need to prove $\mathcal{A} \models \mathsf{Q}$. Let D be a well-founded derivation of Q. We show more generally that for every node of D with label $s' = t'$, we have $\mathcal{A} \models \mathsf{Q}'$ where $\mathsf{Q}' = (\bigwedge_{i\in I} {}^i s = {}^i t) \Longrightarrow s' = t'$. The proof is by well-founded induction.[7] Thus, fix a node of D. If the node is a leaf labelled with one of the premises ${}^j s = {}^j t$ ($j \in I$), then Q′ is the quasiequation $(\bigwedge_{i\in I} {}^i s = {}^i t) \Longrightarrow {}^j s = {}^j t$, which holds in every AIC-structure, so $\mathcal{A} \models \mathsf{Q}'$. Otherwise the node is a point of branching

$$\dfrac{\begin{array}{ccc}\vdots D_l & (\text{for } l, l' \in L) & \vdots D_{l'} \\ \overline{{}^l u = {}^l v} & \cdots & \overline{{}^{l'} u = {}^{l'} v}\end{array}}{s' = t'} \tag{A.46}$$

and, by induction hypothesis, $\mathcal{A}$ satisfies all the quasiequations $(\bigwedge_{i\in I} {}^i s = {}^i t) \Longrightarrow {}^l u = {}^l v$ where $l \in L$. Since (A.46) is a substitution instance of either some axiom of equational logic or of some axiom in Ax, and $\mathcal{A} \models \mathsf{Ax}$, it follows that $\mathcal{A} \models \mathsf{Q}'$.

($\Leftarrow$) Let $\mathsf{Q} = (\bigwedge_{i\in I} {}^i s = {}^i t) \Longrightarrow s = t$ and suppose that $\mathcal{A} \models \mathsf{Q}$ for every AIC-structure $\mathcal{A}$ satisfying Ax. We construct an AIC-structure $\mathcal{A}$ that satisfies the property that if $\mathcal{A} \models \mathsf{Q}$, then $\mathsf{Ax} \vdash_{\mathsf{wf}} \mathsf{Q}$: let $\approx\ \subseteq \mathsf{Terms}^2$ be the relation defined such that $u \approx v$ if and only if $\mathsf{Ax} \vdash_{\mathsf{wf}} (\bigwedge_{i\in I} {}^i s = {}^i t) \Longrightarrow u = v$. Since Ax includes equational logic (fig. 1), $\approx$ is a congruence. This allows us to form the quotient homomorphism $[-]_\approx\colon \mathsf{Terms} \to \mathcal{A}$ where the AIC-structure $\mathcal{A}$ is carried by $A = \mathsf{Terms}/{\approx}$.

[7] Given a well-founded tree T, a property $P(n)$ holds for all nodes n of T whenever the following can be shown: for all nodes n, if $P(m)$ holds for all children m of n, then $P(n)$ holds.

Let us check that $\mathcal{A} \models \mathsf{Ax}$. Let $P = (\bigwedge_{j\in J} {}^j e = {}^j f) \implies e = f$ be an axiom in Ax. Suppose that $\sigma\colon \mathsf{Vars} \to A (= \mathsf{Terms}/{\approx})$ is an interpretation that satisfies ${}^\sigma[\![{}^j e]\!] = {}^\sigma[\![{}^j f]\!]$ for all j. By definition, this means that ${}^j e[\sigma] \approx {}^j f[\sigma]$, which is equivalent to there being a well-founded derivation D_j of $(\bigwedge_{i\in I} {}^i s = {}^i t) \implies {}^j e[\sigma] = {}^j f[\sigma]$, for every $j \in J$. Since $P \in \mathsf{Ax}$, we can then form the derivation

$$\dfrac{\dfrac{\vdots\, D_j}{{}^j e[\sigma] = {}^j f[\sigma]} \quad \overset{(\text{for } j, j' \in J)}{\cdots} \quad \dfrac{\vdots\, D_{j'}}{{}^{j'} e[\sigma] = {}^{j'} f[\sigma]}}{e[\sigma] = f[\sigma]} \tag{A.47}$$

in Ax, where by our definition of a derivation of a quasiequation, each D_j is allowed to have ${}^i s = {}^i t$ show up as a leaf for any $i \in I$. This derivation is well-founded because D_j is well-founded for each $j \in J$.[8] It follows that $\mathsf{Ax} \vdash_{\mathsf{wf}} (\bigwedge_{i\in I} {}^i s = {}^i t) \implies e[\sigma] = f[\sigma]$, and therefore by definition, $e[\sigma] \approx f[\sigma]$ and thus ${}^\sigma[\![e]\!] = {}^\sigma[\![f]\!]$. This proves that $\mathcal{A} \models P$. Since P was an arbitrary axiom of Ax, we conclude that $\mathcal{A} \models \mathsf{Ax}$.

Now, by our assumption that $\mathcal{A} \models \mathsf{Ax}$ implies $\mathcal{A} \models \mathrm{Q}$, we infer that $\mathcal{A} \models \mathrm{Q}$. This means that for any given interpretation $\sigma\colon \mathsf{Vars} \to A$, if ${}^\sigma[\![{}^i s]\!] = {}^\sigma[\![{}^i t]\!]$ for all $i \in I$, then ${}^\sigma[\![s]\!] = {}^\sigma[\![t]\!]$. We can therefore boldly choose $\sigma\colon \mathsf{Vars} \to A$ to be the quotient map restricted to the variables, $\sigma(x) = [x]_\approx$, for which the hypothesis holds trivially: unravelling the definitions, for any $j \in I$, ${}^\sigma[\![{}^j s]\!] = {}^\sigma[\![{}^j t]\!]$ means that ${}^j s \approx {}^j t$, which is the same as saying $\mathsf{Ax} \vdash_{\mathsf{wf}} (\bigwedge_{i\in I} {}^i s = {}^i t) \implies {}^j s = {}^j t$. A derivation D of height 1 exists for this quasiequation, because ${}^j s = {}^j t$ is allowed to appear as a leaf—in particular, as both a leaf and the root. Hence, ${}^\sigma[\![{}^i s]\!] = {}^\sigma[\![{}^i t]\!]$ for each i, and from this we infer that ${}^\sigma[\![s]\!] = {}^\sigma[\![t]\!]$. In other words, $s \approx t$, which is to say that $\mathsf{Ax} \vdash_{\mathsf{wf}} \mathrm{Q}$. □

Completeness of AIC_ω

We are now ready to give the details behind the proof of Theorem 22. We begin with the following result, which is stated without a proof in [33, Proposition 3.3]. Admittedly, we found it less "completely straightforward" than Theunissen and Venema, so we have included a proof for the sake of completeness.

Lemma 47 (Monotone Lifting). *Let N be any lattice. There is a complete lattice L and an order-embedding[9] $m\colon N \hookrightarrow L$ that preserves all meets and joins that exist in N such that for any monotone map $F\colon N \to N$, there is a monotone $\bar{F}\colon L \to L$ such that $\bar{F} \circ m = m \circ F$.*

Proof. The lattice we have in mind is the *Dedekind-MacNeille completion* of N [23], which can be described as follows. For each subset $V \subseteq N$, define

$$V^\Delta = \{x \in N \mid \forall v \in V, v \le x\} \qquad V^\nabla = \{x \in N \mid \forall v \in V, x \le v\}$$

Then the operation $C\colon 2^{|N|} \to 2^{|N|}$ defined $CV = (V^\Delta)^\nabla$ is a closure operation. This gives rise to the complete lattice $L = \{V \in 2^{|N|} \mid V = CV\}$, ordered by set inclusion, and the embedding $m\colon N \to L$ defined $m(v) = C\{v\}$. It is known that the embedding $m\colon N \to L$ preserves all meets and joins that exist in N. It is worth noting that $(-)^\Delta$ and $(-)^\nabla$ are both antitone, and that this implies that $C = (-)^\nabla \circ (-)^\Delta$ is monotone.

Now let $F\colon N \to N$ be a monotone map. We extend F to L by defining $\bar{F}\colon L \to L$ by $\bar{F}(V) = C(F[V])$. The operation $\bar{F}$ is clearly monotone. We are left with showing that $\bar{F} \circ m = m \circ F$. Observe that for any $v \in N$,

$$\begin{aligned} m(v) = C\{v\} = (\{v\}^\Delta)^\nabla &= \{x \in N \mid \forall y \in \{v\}^\Delta, x \le y\} \\ &= \{x \in N \mid \forall y \in {\uparrow} v, x \le y\} = \{x \in N \mid x \le v\} = {\downarrow} v \end{aligned}$$

The second to last equality can be seen by taking $y = v$. In particular, $m \circ F(v) = C\{F(v)\} = {\downarrow} F(v)$ for any $v \in N$. On the other side, we have

$$\bar{F} \circ m(v) = CF[C\{v\}] = CF[{\downarrow} v] = C\{F(x) \mid x \le v\}$$

Therefore, our goal is to show that $C\{F(x) \mid x \le v\} = {\downarrow} F(v)$. This will happen in two parts, one for each inclusion.

Given any $x \le v$, by monotonicity we see that $F(x) \le F(v)$. It follows that $\{F(x) \mid x \le v\} \subseteq {\downarrow} F(v)$. Since ${\downarrow} F(v) \in L$, by monotonicity of C we have

$$C\{F(x) \mid x \le v\} \subseteq C({\downarrow} F(v)) = {\downarrow} F(v)$$

This establishes one inclusion.

For the opposite inclusion, let $y \le F(v)$. We want to show that $y \in C\{F(x) \mid x \le v\} = (\{F(x) \mid x \le v\}^\Delta)^\nabla$, which is equivalent to the statement that *for any $u \in N$ such that $F(x) \le u$ for all $x \le v$, we have $y \le u$*. So, let $u \in N$ such that $F(x) \le u$ for all $x \le v$. Then in particular, $F(v) \le u$. But $y \le F(v)$. This tells us that $y \le u$, so $y \in C\{F(x) \mid x \le v\}$ as desired. □

Theorem 22 (AIC_ω-Embedding). *Let $\mathcal{A}_0 \models \mathsf{AIC}_\omega$ be an AIC-structure. Then there exists a complete lattice $(L, \sqsubseteq)$ and a sequence algebra $\mathcal{A}$ carried by L^ω such that $\mathcal{A}_0$* embeds *into $\mathcal{A}$, in the sense that there exists an injective algebra homomorphism $\varepsilon\colon \mathcal{A}_0 \hookrightarrow \mathcal{A}$.*

[8] We feel it is important to note that this is where well-foundedness plays a role. If we instead altered our definition of derivation to require *finite height* instead of well-foundedness, then this step no longer goes through: if the set of derivations D_j has no upper bound on their heights (say, $J = \omega$ and the height of D_j is j like in **??**), then we could no longer form the derivation in (A.47).

[9] A monotone map between posets $f\colon X \to Y$ is an *order-embedding* if for any $x, x' \in X$, $x \le x'$ if and only if $f(x) \le f(x')$. Order-embedding maps are necessarily injective, and surjective order-embeddings are order isomorphisms.

Proof. Start by constructing the *lattice of heads*,

$$L_0 = \left\{ \circledcirc^{\mathcal{A}_0} a \;\middle|\; a \in A_0 \right\}$$

This is a lattice with lattice operations interpreted as

$$\bot^{L_0} = \circledcirc^{\mathcal{A}_0} \bot^{\mathcal{A}_0} \qquad \top^{L_0} = \circledcirc^{\mathcal{A}_0} \top^{\mathcal{A}_0}$$
$$(\circledcirc^{\mathcal{A}_0} a) \sqcap^{L_0} (\circledcirc^{\mathcal{A}_0} b) = \circledcirc^{\mathcal{A}_0} (a \wedge^{\mathcal{A}_0} b) \qquad (\circledcirc^{\mathcal{A}_0} a) \sqcup^{L_0} (\circledcirc^{\mathcal{A}_0} b) = \circledcirc^{\mathcal{A}_0} (a \vee^{\mathcal{A}_0} b)$$

because $\circledcirc^{\mathcal{A}_0}$ commutes with the lattice operations (see Table 3). This allows us to further define the lattice homomorphism $e' : A_0 \to L_0^\omega$ given by

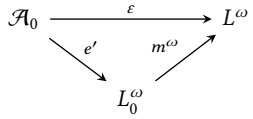
$$e'(a)(n) = \circledcirc^{\mathcal{A}_0} (\bigcirc^{\mathcal{A}_0})^n a$$

where $(\bigcirc^{\mathcal{A}_0})^n$ is the n-fold application of the shift operation. That e' is a lattice homomorphisms folllows from the Head and Shift axioms, which ensure the the $\circledcirc$ and $\bigcirc$ operations preserve commute with the lattice structure. It follows directly from the first sequence axiom in Table 3 that e' is injective. Note that the function operations $F^{\mathcal{A}_0}$ for $F \in \mathsf{Funcs}$ restrict to L_0, since $F^{\mathcal{A}_0} \circledcirc a = \circledcirc F^{\mathcal{A}_0} a$.

By Lemma 47, there is a complete lattice L and an order-embedding $m : L_0 \hookrightarrow L$ such that every monotone operation $G : L_0 \to L_0$ extends to a monotone operation $\bar{G} : L \to L$. Write $m^\omega : L_0^\omega \to L^\omega$ for the pointwise embedding defined by $m^\omega(\sigma)(n) = m(\sigma(n))$ for any $\sigma \in L_0^\omega$ and $n \in \omega$. We obtain a sequence algebra $\mathcal{A}$ carried by L^ω by lifting each operation $F^{\mathcal{A}_0} : L_0 \to L_0$ to a monotone operation $\bar{F}$ on L and applying it pointwise to sequences to obtain the unary operation $F^{\mathcal{A}} : L^\omega \to L^\omega$.

From here on, most superscripts indicating the type of the operations will be supressed, since they can be inferred from context.

Finally, let $\varepsilon = m^\omega \circ e'$. We obtain the following diagram:



$$\varepsilon(a)(n) = m^\omega \circ e'(a)(n) = m(\circledcirc \bigcirc^n a)$$

It follows from the injectivity of m^ω and e' that ε is injective. It now suffices to see that ε is a homomorphism of AIC-structures.

Lattice Since m is a lattice homomorphism, so is the pointwise application m^ω. Therefore ε is a lattice homomorphism, being the composite of the lattice homomorphisms e' and m^ω.

Head Given $a \in A_0$, we have

$$\begin{aligned}
\varepsilon(\circledcirc a)(n) &= m(\circledcirc \bigcirc^n \circledcirc a) \\
&= m(\circledcirc \circledcirc a) && \text{(Head)} \\
&= m(\circledcirc a) && \text{(Head)} \\
&= \varepsilon(a)(0) && \text{(definition of } \varepsilon\text{)} \\
&= (\circledcirc \varepsilon(a))(n) && \text{(sequence algebra)}
\end{aligned}$$

Shift Given $a \in A_0$, we have

$$\begin{aligned}
\varepsilon(\bigcirc a)(n) &= m(\circledcirc \bigcirc^n \bigcirc a) \\
&= m(\circledcirc \bigcirc^{n+1} a) \\
&= \varepsilon(a)(n+1) && \text{(definition of } \varepsilon\text{)} \\
&= (\bigcirc \varepsilon(a))(n) && \text{(sequence algebra)}
\end{aligned}$$

Functions Given $a \in A_0$ and $F \in \mathsf{Funcs}$, we have

$$\begin{aligned}
\varepsilon(Fa)(n) &= m(\circledcirc \bigcirc^n Fa) \\
&= m(\circledcirc F \bigcirc^n a) && \text{(Shift)} \\
&= m(F \circledcirc \bigcirc^n a) && \text{(Head)} \\
&= \bar{F}(m(\circledcirc \bigcirc^n a)) && (\bar{F} \text{ extends } F) \\
&= \bar{F}(\varepsilon(a)(n)) && \text{(definition of } \varepsilon\text{)} \\
&= (F^{\mathcal{A}} \varepsilon(a))(n) && \text{(sequence algebra)}
\end{aligned}$$

Iteration Given $a \in A_0$ and $F \in \mathsf{Funcs}$, we have

$$\begin{aligned}
\varepsilon(F^* a)(n) &= m(\circledcirc \bigcirc^n F^* a) \\
&= m(\circledcirc F^n F^* \bigcirc^n a) && \text{(Shift)} \\
&= m(F^n \circledcirc F^* \bigcirc^n a) && \text{(Head)} \\
&= m(F^n \circledcirc \bigcirc^n a) && \text{(Head)} \\
&= \bar{F}^n \circ m(\circledcirc \bigcirc^n a) && (\bar{F} \text{ lifts } F^{\mathscr{A}_0}) \\
&= \bar{F}^n(\varepsilon(a)(n)) && \text{(definition of } \varepsilon) \\
&= ((F^*)^{\mathscr{A}} \varepsilon(a))(n) && \text{(sequence algebra)}
\end{aligned}$$

Majorum/Minorum We will just do the majorum case (tail-suprema), because the minorum case is symmetric. We begin with the following observation: for any $k \in \omega$ and $c \in A_0$, by the Maj/Minorum and Shift axioms, $\bigcirc^k \Diamond c \sqsubseteq \Diamond c$. We therefore have $\circledcirc \bigcirc^k \Diamond c \sqsubseteq \circledcirc \Diamond c$ for all $k \in \omega$. The Sequence axioms now tell us that $\circledcirc \Diamond c$ is the *least* upper bound of $\{\circledcirc \bigcirc^k c \mid k \in \omega\}$, and that this least upper bound exists in L_0. Now, if we let $c = \bigcirc^n a$, we see that

$$\begin{aligned}
\circledcirc \Diamond \bigcirc^n a &= \bigsqcup_{k \geq 0} \circledcirc \bigcirc^k \bigcirc^n a \\
&= \bigsqcup_{k \geq 0} \circledcirc \bigcirc^{n+k} a \\
&= \bigsqcup_{k \geq n} \circledcirc \bigcirc^k a
\end{aligned}$$

Since m preserves all suprema that exist in L_0, we can derive

$$\begin{aligned}
\varepsilon(\Diamond a)(n) &= m(\circledcirc \bigcirc^n \Diamond a) \\
&= m(\circledcirc \Diamond \bigcirc^n a) && \text{(Shift)} \\
&= m\Big(\bigsqcup_{k \geq n} \circledcirc \bigcirc^k a\Big) && (\circledcirc \Diamond a \text{ a least upper bound}) \\
&= \bigsqcup_{k \geq n} m(\circledcirc \bigcirc^k a) && (m \text{ preserves joins}) \\
&= \bigsqcup_{k \geq n} \varepsilon(a)(k) && \text{(definition of } \varepsilon) \\
&= (\Diamond \varepsilon(a))(k) && \text{(sequence algebra)}
\end{aligned}$$

Hence, ε is an algebra homomorphism. This completes the proof of the embedding theorem. □

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009; revised 20 February 2007; revised 12 March 2009; accepted 5 June 2009