Universität Augsburg

Non-Associative Kleene Algebra and Temporal Logics

Jules Desharnais and Bernhard Möller

Report 2016-08 December 2016

Institut für Informatik
D-86135 Augsburg

Copyright © Jules Desharnais and Bernhard Möller
Institut für Informatik
Universität Augsburg
D–86135 Augsburg, Germany
http://www.Informatik.Uni-Augsburg.DE
— all rights reserved —

Non-Associative Kleene Algebra and Temporal Logics

Jules Desharnais[1] and Bernhard Möller[2]

[1] Université Laval, Québec, Canada
[2] Institut für Informatik, Universität Augsburg, Germany

Abstract. In earlier papers we have presented algebraic semantics of CTL and CTL*. However, they were not fully satisfactory. In particular, the treatment of the iteration operators U ("Until") and W ("While") employed ad-hoc definitions with general recursion, and their interrelation in CTL* and CTL was not set up in a very algebraic way. In this paper we use a new operator with which U and W can be described by variants of the Kleene star and omega iteration. However, the operator is neither associative nor does it have a neutral element. Therefore we present a general investigation of the star and omega for such operators in what we call iteration algebras. The relation between various semantics for CTL* and CTL can then be expressed by homomorphisms between iteration algebras, which is more satisfactory than the original approach.

Keywords: temporal logics, semantics, Kleene algebra, iteration algebra

1 Introduction

The temporal logic CTL^* and its sublogics CTL and LTL are prominent tools in the analysis of concurrent and reactive systems. Although they are by now well understood, one still rarely finds algebraic treatments of their semantics. In the present paper we take up the approach of [18] and refine it in several ways. First, we present a variant of Kleene algebra where the underlying multiplication is not assumed to be associative. Such an operator arises, e.g., in the semantics of the until operator of CTL^* and its relatives. Therefore we present a general investigation of the star and omega for such operators in what we call iteration algebras. The relation between various semantics for CTL* and CTL can then be expressed by homomorphisms between iteration algebras; in particular, several tedious ad-hoc applications of the principle of least/greatest fixed point fusion that occurred in [18] are now replaced by a single proof for general iteration algebras. Another new feature is a much cleaner separation between finite and infinite traces than in the predecessor paper. Also a number of new results concerning the universal path quantifier A and the globality operator G arise. For lack of space all proofs are omitted; they are found in the report [4].

2 Modelling CTL^*

Formulas in CTL^* characterise sets of traces, where a trace is a finite or infinite sequence of program states. A set Φ of *atomic propositions* is used to distinguish sets of states. The syntax of the language Ψ of *CTL^* formulas* (see e.g. [7]) over Φ is given by the grammar

$$\Psi \ ::= \ \bot \mid \Phi \mid \Psi \to \Psi \mid \mathsf{E}\Psi \mid \mathsf{X}\,\Psi \mid \Psi\,\mathsf{U}\,\Psi \ ,$$

where $\bot$ denotes falsity, $\to$ is logical implication, E is the existential quantifier on paths, and X and U are the next-time and until operators.

Let us briefly recall the informal semantics. A trace is said to satisfy an atomic formula iff its first state does. A path σ satisfies $\mathsf{E}\varphi$ iff there is a path τ that satisfies φ and has the same first state as σ. The formula $\mathsf{X}\varphi$ is true for a trace σ if φ is true for the remainder of σ after one step. A trace σ satisfies $\varphi\,\mathsf{U}\,\psi$ iff after a finite number (including zero) of X steps within σ the remaining trace satisfies ψ and all intermediate trace pieces for which ψ does not yet hold satisfy φ.

The logical connectives $\neg$, $\wedge$, $\vee$, A are defined, as usual, by $\neg\varphi =_{df} \varphi \to \bot$, $\top =_{df} \neg\bot$, $\varphi \wedge \psi =_{df} \neg(\varphi \to \neg\psi)$, $\varphi \vee \psi =_{df} \neg\varphi \to \psi$ and $\mathsf{A}\varphi =_{df} \neg\,\mathsf{E}\neg\varphi$. Moreover, the "finally" operator F and the "globally" operator G are defined by

$$\mathsf{F}\psi =_{df} \top\mathsf{U}\psi \qquad \text{and} \qquad \mathsf{G}\psi =_{df} \neg\mathsf{F}\neg\psi \ .$$

Informally, $\mathsf{F}\psi$ holds if after a finite number of steps the remainder of the trace satisfies ψ, while $\mathsf{G}\psi$ holds if after every finite number of steps ψ still holds.

The sublanguages Ξ of *state formulas*[3] that denote sets of states and Π of *path formulas* that denote sets of computation traces are given by

$$\begin{aligned} \Xi &::= \bot \mid \Phi \mid \Xi \to \Xi \mid \mathsf{E}\Pi \ , \\ \Pi &::= \Xi \mid \Pi \to \Pi \mid \mathsf{X}\,\Pi \mid \Pi\,\mathsf{U}\,\Pi \ . \end{aligned}$$

To motivate our algebraic semantics, we briefly recapitulate the standard CTL^* semantics of formulas. Its basic objects are traces σ from Σ^ω, the set of infinite sequences of states from some set Σ. The i-th element of σ (indices starting with 0) is denoted σ_i, and σ^i is the trace that results from σ by removing its first i elements. Hence $\sigma^0 = \sigma$.

Each atomic proposition $\pi \in \Phi$ is associated with the set $\Sigma_\pi \subseteq \Sigma$ of states for which π is true. The relation $\sigma \models \varphi$ of *satisfaction* of a formula φ by a trace σ is defined inductively (see e.g. [7]) by

$$\begin{array}{lll} \sigma \not\models \bot \ , & & \\ \sigma \models \pi & \text{iff } \sigma_0 \in \Sigma_\pi \ , & \\ \sigma \models \varphi \to \psi & \text{iff } \sigma \models \varphi \text{ implies } \sigma \models \psi \ , & \end{array}
\qquad
\begin{array}{ll} \sigma \models \mathsf{E}\varphi & \text{iff } \exists\,\tau : \tau_0 = \sigma_0 \text{ and } \tau \models \varphi \ , \\ \sigma \models \mathsf{X}\,\varphi & \text{iff } \sigma^1 \models \varphi \ , \\ \sigma \models \varphi\,\mathsf{U}\,\psi & \text{iff } \exists\, j \geq 0 :\ \sigma^j \models \psi \text{ and} \\ & \quad \forall\, k < j :\ \sigma^k \models \varphi \ . \end{array}$$

[3]In the literature this set is usually called Σ. We avoid this, since throughout the paper we use Σ for sets of states.

In particular, $\sigma \models \neg\varphi$ iff $\sigma \not\models \varphi$.

We quickly repeat the proof of validity of the CTL^* axiom

$$\neg\mathsf{X}\varphi \leftrightarrow \mathsf{X}\neg\varphi \ , \tag{1}$$

since this will be crucial for the algebraic representation of X in Sect. 6:

$$\sigma \models \neg\mathsf{X}\varphi \ \Leftrightarrow\ \sigma \not\models \mathsf{X}\varphi \ \Leftrightarrow\ \sigma^1 \not\models \varphi \ \Leftrightarrow\ \sigma^1 \models \neg\varphi \ \Leftrightarrow\ \sigma \models \mathsf{X}\neg\varphi \ .$$

3 Semirings, Quantales, Fixed Points and Iteration

We formulate our more abstract developments in terms of algebraic structures. The elements of these structures may, for instance, stand for sets of traces.

Definition 3.1

1. An *idempotent left semiring*, briefly IL-semiring, is a structure $(A, +, \cdot, 0, 1)$ such that $(A, +, 0)$ is a commutative monoid with idempotent addition, that is, $(A, \cdot, 1)$ is a monoid, multiplication distributes from the right over addition and 0 is a left annihilator for multiplication, that is, $0 \cdot a = 0$ for all $a \in A$. An IL-semiring is *left-distributive* if multiplication distributes over addition also from the left.
2. Every IL-semiring can be partially ordered by setting $a \leq b \Leftrightarrow_{df} a + b = b$. Then $+$ and $\cdot$ are isotone w.r.t. $\leq$ and 0 is the least element. Moreover, $a+b$ is the supremum of $a, b \in A$. An IL-Semiring is *bounded* if it has a greatest element $\top$.
3. An IL-semiring is called a *left quantale* [15] if $\leq$ induces a complete lattice and multiplication distributes over arbitrary suprema from the right. The infimum and the supremum of a subset $B \subseteq A$ are denoted by $\bigsqcap B$ and $\bigsqcup B$, respectively. Their binary variants are $a \sqcap b$ and $a \sqcup b$ (the latter coinciding with $a + b$).
4. In left quantales finite and infinite iteration can be defined as least and greatest fixed points, namely $a^* =_{df} \mu x \,.\, 1 + a \cdot x$ and $a^\omega =_{df} \nu x \,.\, a \cdot x$. For details and properties see the appendix in Sect. 13 and [15].
5. The IL-semiring/left quantale is *Boolean* if $(A, \leq)$ induces a Boolean algebra. In this case we define $a - b =_{df} a \sqcap \overline{b}$.

Quantales (or *standard Kleene algebras* [2]) have been used in many contexts other than that of program semantics (cf. the general reference [19]). They have the advantage that the general fixpoint calculus is available there. A number of our proofs need the principle of fixpoint fusion which is a second-order principle; in the first-order setting of conventional Kleene algebras [14] only special cases of it, like the induction and coinduction rules, can be used as axioms.

Example 3.2 We want to use an algebra of sets of traces. We set $\Sigma^\infty =_{df} \Sigma^+ \cup \Sigma^\omega$, where Σ^+ is the set of non-empty finite traces over Σ. The operator .

denotes concatenation of traces. First we define the partial operation of the *fusion product* that glues traces together at a common point, if any. For $\sigma, \tau \in \Sigma^\infty$,

$$\sigma \bowtie \tau = \begin{cases} \sigma & \text{if } \sigma \in \Sigma^\omega \ , \\ \sigma'.x.\tau' & \text{if } \sigma \in \Sigma^+, \sigma = \sigma'.x, \tau = x.\tau' \text{ for some } x \in \Sigma \ , \\ \text{undefined} & \text{otherwise} \ . \end{cases}$$

The *purely infinite* and *purely finite* parts of a set U of traces are $\mathsf{inf}\, U =_{df} U \cap \Sigma^\omega$ and $\mathsf{fin}\, U =_{df} U - \mathsf{inf}\, U$. With this we extend $\bowtie$ to trace sets U, V as

$$U \bowtie V =_{df} \mathsf{inf}\, U \cup \{s \bowtie t : s \in \mathsf{fin}\, U \wedge t \in V\} \ .$$

This operation has the set Σ, viewed as a set of one-element traces, as its neutral element. Moreover, $U \bowtie \emptyset = \mathsf{inf}\, U$ and hence $U \bowtie \emptyset = \emptyset$ iff $\mathsf{inf}\, U = \emptyset$. This will be generalised in Sect. 7.

Now we define the Boolean left quantale $\mathsf{TRC}(\Sigma)$ of sets of finite and infinite traces by $\mathsf{TRC}(\Sigma) =_{df} (\mathcal{P}(\Sigma^\infty), \cup, \bowtie, \emptyset, \Sigma)$. This quantale is even left-distributive. A transition relation over a state set Σ can be modelled in $\mathsf{TRC}(\Sigma)$ as a set R of traces of length 2. The powers R^i of R consist of traces of length $i + 1$ that are generated by R-transitions. In particular, we instantiate R to $\mathrm{NX} =_{df} \Sigma.\Sigma$, the set of all two-state traces and hence the most general next-step transition relation. Then $\mathsf{TRC}(\Sigma)$ is generated by NX as $\mathsf{TRC}(\Sigma) = \mathrm{NX}^* \cup \mathrm{NX}^\omega$. This is generalised to Boolean left quantales in Sect. 8. □

Next to an abstract representation of sets of traces we will also need one for sets of states. This is achieved by the notion of tests [13].

Definition 3.3 A *test* in an IL-semiring is an element p that has a complement $\neg p$ w.r.t. the multiplicative unit 1, namely $p + \neg p = 1$ and $p \cdot \neg p = 0 = \neg p \cdot p$. The set of all tests in A is denoted by $\mathsf{test}(A)$.

The element $\neg p$ is uniquely determined by these axioms if it exists. In a Boolean IL-semiring every element $p \leq 1$ is a test with $\neg p = \overline{p} \sqcap 1$.

The multiplicative identity Σ has exactly the subsets of Σ as its sub-objects, hence in $\mathsf{TRC}(\Sigma)$ the tests faithfully represent sets of states.

The expressions $p \cdot a$ and $a \cdot p$ abstractly represent restriction of the traces in a to the ones that start and end in p-states, resp.

Using tests we can also define a domain operator and the modal operators diamond and box (cf. [5]).

Definition 3.4 Consider a bounded IL-semiring A and $a \in A, q \in \mathsf{test}(A)$. The *domain operator* $\ulcorner : S \to \mathsf{test}(S)$ is axiomatised by the Galois connection

$$\ulcorner a \leq q \Leftrightarrow a \leq q \cdot \top \ . \tag{2}$$

Then $|a\rangle q =_{df} \ulcorner(a \cdot q)$ and $|a] =_{df} \neg|a\rangle\neg a$.

In $\mathsf{TRC}(\Sigma)$, for trace set U the domain $\ulcorner U$ consists of all starting states of traces in U. Moreover $|U\rangle P$ for some set $P \subseteq \Sigma$ is the set of all starting states of traces in U that end in some state in P, hence a kind of inverse image of P under U. Dually, $|U]P$ consists of those states x for which all traces in U starting in x have their final states, if any, in P.

We recall a few basic properties of tests, domain and restriction; see [15,5].

Lemma 3.5 *Let S be a bounded IL-semiring, $a, b \in S$ and $p, q \in \mathsf{test}(S)$.*

1. *By the Galois connection* (2) *domain preserves all existing suprema and hence is isotone (see [8]).*
2. $\ulcorner a = 0 \Leftrightarrow a = 0$.
3. $a = \ulcorner a \cdot a$ *and* $\ulcorner(p \cdot a) \leq p$.
4. $\ulcorner(p \cdot \top) = p$.
5. $\ulcorner(a \cdot b) = \ulcorner(a \cdot \ulcorner b)$. *This property, called* locality*, means that the domain of a composition does not depend on the inner structure of the second operand, but only on its starting states.*
6. $p \leq q \Leftrightarrow p \cdot \top \leq q \cdot \top$.
7. *If $a \sqcap b$ exists then $p \cdot (a \sqcap b) = p \cdot a \sqcap b = a \sqcap p \cdot b$. Hence if $b \leq a$ then $p \cdot a \sqcap b = p \cdot b$. In particular, $p \cdot \top \sqcap b = p \cdot b$.*
8. *If S is Boolean then $\neg p \cdot \top = \overline{p \cdot \top}$.*
9. $|a \cdot b\rangle q = |a\rangle(|b\rangle q)$ *and* $|a \cdot b]q = |a](|b]q)$.
10. $p \cdot |b\rangle q = |p \cdot b\rangle q$ *(import/export).*
11. $p + |a\rangle q \leq q \Rightarrow |a^*\rangle p \leq q$ *and* $p \leq q \cdot |a]p \Rightarrow p \leq |a^*]q$ *(diamond/box star induction).*

By these properties we can represent the set of all possible paths that start with some state in set p by the *test ideal* $p \cdot \top$. By Part 6 the set of test ideals is isomorphic to the set of tests.

4 General Algebraic Semantics of CTL^*

We now give our algebraic interpretation of CTL^* over a Boolean left quantale S. As a preparation we transform the semantics from Sect. 2 into a set-based one by assigning to each formula φ the set $[\![\varphi]\!] =_{df} \{\sigma \mid \sigma \models \varphi\}$ of paths that satisfy it.

$$
\begin{aligned}
[\![\bot]\!] &= \emptyset \ , & [\![\mathsf{E}\varphi]\!] &= \ulcorner[\![\varphi]\!] \bowtie \Sigma^\omega \ , \\
[\![\mathsf{X}\,\varphi]\!] &= \mathrm{NX} \bowtie [\![\varphi]\!] \ , & [\![\pi]\!] &= \Sigma_\pi \bowtie \Sigma^\omega \ , \\
[\![\varphi \to \psi]\!] &= \overline{[\![\varphi]\!]} \cup [\![\psi]\!] \ , & [\![\varphi \,\mathsf{U}\, \psi]\!] &= \bigcup_{j \geq 0} (\mathrm{NX}^j \bowtie [\![\psi]\!] \cap \bigcap_{k<j} \mathrm{NX}^k \bowtie [\![\varphi]\!]) \ .
\end{aligned}
$$

In this set-based semantics, every atomic proposition $\pi \in \Phi$ is algebraically associated with a set $\Sigma_\pi \subseteq \Sigma$ of states, i.e., with an element of $\mathsf{test}(\mathsf{TRC}(\Sigma))$. Therefore, to save some notation, in the algebraic semantics we simply set $\Phi = \mathsf{test}(S)$. Moreover, we fix an element n (n standing for "next" and corresponding to NX) that represents the transition system underlying the logic. The precise requirements for n will be discussed in Sect. 6. Then the concrete semantics above generalises to a function $[\![\_]\!] : \Psi \to S$, where $[\![\varphi]\!]$ abstractly represents the set of paths satisfying formula φ.

Definition 4.1 The *general algebraic semantics* $[\![\varphi]\!]$ of CTL^* formula φ is defined inductively over the structure of φ. This results from the set-based semantics by a straightforward translation of the concrete operators of $\mathsf{TRC}(\Sigma)$ into the corresponding quantale operators:

$$
\begin{aligned}
[\![\bot]\!] &= 0 \ , & [\![\mathsf{E}\varphi]\!] &= {}^{\ulcorner}[\![\varphi]\!] \cdot \top \ , \\
[\![p]\!] &= p \cdot \top \ , & [\![\mathsf{X}\,\varphi]\!] &= \mathsf{n} \cdot [\![\varphi]\!] \ , \\
[\![\varphi \to \psi]\!] &= \overline{[\![\varphi]\!]} + [\![\psi]\!] \ , & [\![\varphi \,\mathsf{U}\, \psi]\!] &= \bigsqcup_{j \geq 0} (\mathsf{n}^j \cdot [\![\psi]\!] \sqcap \bigsqcap_{k<j} \mathsf{n}^k \cdot [\![\varphi]\!]) \ .
\end{aligned}
$$

As a word of warning, the definition $[\![p]\!] = p \cdot \top$ does not correspond exactly to the TRC semantics, where $[\![\pi]\!] = \Sigma_\pi \bowtie \Sigma^\omega$ and $\Sigma^\omega \neq \top$. This problem will be taken up in Sect. 7.

Using the above definitions, it is easy to check that

$$
[\![\varphi \vee \psi]\!] = [\![\varphi]\!] + [\![\psi]\!] \ , \ [\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \sqcap [\![\psi]\!] \ , \ [\![\neg\varphi]\!] = \overline{[\![\varphi]\!]} \ , \ [\![\top]\!] = \top \ . \qquad (3)
$$

Then the above semantics coincides with that of Sect. 2, as far as infinite streams are concerned. This is discussed in detail in Sects. 6 and 7.

To exemplify our semantics we prove a number of properties of the path quantifiers. In particular, we work out a more explicit form of the A semantics.

Corollary 4.2 $[\![\mathsf{EE}\psi]\!] = [\![\mathsf{E}\psi]\!]$ *and* $[\![\mathsf{AA}\psi]\!] = [\![\mathsf{A}\psi]\!]$ *and* $[\![\mathsf{A}\psi]\!] = \neg{}^{\ulcorner}\overline{[\![\psi]\!]} \cdot \top$.

Proof.

1. For the first equation, by the definition of $[\![\,]\!]$ twice, Lm. 3.5.4 and the definition of $[\![\,]\!]$ again,

$$
[\![\mathsf{EE}\psi]\!] = {}^{\ulcorner}[\![\mathsf{E}\psi]\!] \cdot \top = {}^{\ulcorner}({}^{\ulcorner}[\![\psi]\!] \cdot \top) \cdot \top = {}^{\ulcorner}[\![\psi]\!] \cdot \top = [\![\mathsf{E}\psi]\!] \ .
$$

The second equation is immediate from that and the definition of A.

2. By the definitions of A, $\neg$ and E, and Lm. 3.5.8,

$$
[\![\mathsf{A}\psi]\!] = [\![\neg\mathsf{E}\neg\psi]\!] = \overline{[\![\mathsf{E}\neg\psi]\!]} = \overline{{}^{\ulcorner}[\![\neg\psi]\!] \cdot \top} = \neg{}^{\ulcorner}\overline{[\![\psi]\!]} \cdot \top \ .
$$

□

This entails a number of further properties of E and A.

Lemma 4.3 *For atomic proposition p and arbitrary formulas φ, ψ,*

$$
\begin{aligned}
[\![\mathsf{E}\bot]\!] &= 0 \ , & [\![\mathsf{A}\bot]\!] &= 0 \ , \\
[\![\mathsf{E}\top]\!] &= \top \ , & [\![\mathsf{A}\top]\!] &= \top \ , \\
[\![\mathsf{E}p]\!] &= [\![p]\!] \ , & [\![\mathsf{A}p]\!] &= [\![p]\!] \ , \\
[\![\mathsf{E}(\varphi \vee \psi)]\!] &= [\![\mathsf{E}\varphi]\!] + [\![\mathsf{E}\psi]\!] \ , & [\![\mathsf{A}(p \vee \psi)]\!] &= [\![p]\!] + [\![\mathsf{A}\psi]\!] \ , \\
[\![\mathsf{E}(p \wedge \psi)]\!] &= p \cdot [\![\mathsf{E}\psi]\!] \ , & [\![\mathsf{A}(\varphi \wedge \psi)]\!] &= [\![\mathsf{A}\varphi]\!] \sqcap [\![\mathsf{A}\psi]\!] \ .
\end{aligned}
$$

In particular,

$$[\![\mathsf{E}(p \vee \varphi)]\!] = [\![p]\!] + [\![\mathsf{E}\varphi]\!] \ , \qquad [\![\mathsf{A}(p \wedge \varphi)]\!] = p \cdot [\![\mathsf{A}\varphi]\!] \ .$$

We only show the properties for E; the ones for A are immediate from those by De Morgan duality and domain algebra.

The first two properties follow from the definition of $[\![\,]\!]$, (3) and $\ulcorner\top = 1$ with neutrality of 1. Next, by definition of $[\![\,]\!]$ twice, Lm. 3.5.4 and definition of $[\![\,]\!]$ again,

$$[\![\mathsf{E}p]\!] = \ulcorner[\![p]\!] \cdot \top = \ulcorner(p \cdot \top) \cdot \top = p \cdot \top = [\![p]\!] \ .$$

Further, by definition of $[\![\,]\!]$, (3), disjunctivity of domain, distributivity and definition of $[\![\,]\!]$ again,

$$\begin{aligned}[\![\mathsf{E}(\varphi \vee \psi)]\!] &= \ulcorner([\![(\varphi \vee \psi)]\!]) \cdot \top = \ulcorner([\![\varphi]\!] + [\![\psi]\!]) \cdot \top = (\ulcorner[\![\varphi]\!] + \ulcorner[\![\varphi]\!]) \cdot \top \\ &= \ulcorner[\![\varphi]\!] \cdot \top + \ulcorner[\![\varphi]\!] \cdot \top = [\![\mathsf{E}\varphi]\!] + [\![\mathsf{E}\psi]\!] \ .\end{aligned}$$

Moreover, by definition of $[\![\,]\!]$, (3), definition of $[\![\,]\!]$, Lm. 3.5.7, import/export (Lm. 3.5.10) and definition of $[\![\,]\!]$ again,

$$\begin{aligned}[\![\mathsf{E}(p \wedge \varphi)]\!] &= \ulcorner[\![(p \wedge \varphi)]\!] \cdot \top = \ulcorner([\![p]\!] \sqcap [\![\varphi]\!]) \cdot \top = \ulcorner(p \cdot \top \sqcap [\![\varphi]\!]) \cdot \top \\ &= \ulcorner(p \cdot [\![\varphi]\!]) \cdot \top = p \cdot \ulcorner[\![\varphi]\!] \cdot \top = p \cdot [\![\mathsf{E}\varphi]\!] \ .\end{aligned}$$

The remaining property is immediate from the third and fourth ones. ☐

Moreover, for the CTL^* axiom $\mathsf{EX}\top$[7] we obtain the following result.

Lemma 4.4 $[\![\mathsf{EX}\top]\!] = \top \Leftrightarrow \ulcorner\mathsf{n} = 1 \Leftrightarrow \mathsf{n}$ *total.*

Proof. This follows by Lm. 3.5.6, since by Def. 4.1 and Lm. 3.5.4, $[\![\mathsf{EX}\top]\!] = \ulcorner(\mathsf{n} \cdot \top) \cdot \top = \ulcorner\mathsf{n} \cdot \top$. ☐

5 Modified Iteration and the Semantics of Until

We now deal with the semantics of the until operator. To bring the corresponding expression in Def. 4.1 into more palatable shape we introduce a bit of notation. For elements $a, b \in S$ and $j \in \mathbb{N}$ we set

$$a \boxed{j}\, b =_{df} \mathsf{n}^j \cdot b \sqcap \prod_{k<j} \mathsf{n}^k \cdot a \ , \tag{4}$$

which is the expression occurring in the right hand side of the semantic equation for $[\![\varphi \,\mathsf{U}\, \psi]\!]$ when $a = [\![\varphi]\!]$ and $b = [\![\psi]\!]$. It states that a holds j times and then ψ holds. The idea is now to find an inductive formulation of $\boxed{j}$ driven by j. For the induction base we calculate, using the definitions of $\boxed{0}$ and powers, neutrality of 1 and lattice algebra, $a \boxed{0}\, b = \mathsf{n}^0 \cdot b \sqcap \prod_{k<0} \mathsf{n}^k \cdot a = b \sqcap \top = b$. To proceed with the induction step we need an assumption about n that is closely related to (1), as is discussed in detail in Sect. 6. This condition reads

$$\forall\, a, b \in S : \mathsf{n} \cdot (a \sqcap b) = \mathsf{n} \cdot a \sqcap \mathsf{n} \cdot b \ . \tag{LDM}$$

It means that left multiplication by n distributes through binary and hence non-empty finite meets. With that we calculate as follows. By definition, splitting the $\bigsqcap$ expression, definition of powers and neutrality of 1, commutativity of $\sqcap$, index shift, (LDM), definition of $\boxed{j}$, and the definition below:

$$\begin{array}{ll} & a \boxed{j+1} b \\ = & \mathsf{n}^{j+1} \cdot b \sqcap \bigsqcap_{k<j+1} \mathsf{n}^k \cdot a \\ = & \mathsf{n}^{j+1} \cdot b \ \sqcap \ \mathsf{n}^0 \cdot a \sqcap \bigsqcap_{k=1}^{j} \mathsf{n}^k \cdot a \\ = & a \sqcap \mathsf{n} \cdot \mathsf{n}^j \cdot b \sqcap \bigsqcap_{k=1}^{j} \mathsf{n} \cdot \mathsf{n}^{k-1} \cdot a \\ = & a \sqcap \mathsf{n} \cdot \mathsf{n}^j \cdot b \sqcap \bigsqcap_{l<j} \mathsf{n} \cdot \mathsf{n}^l \cdot a \\ = & a \sqcap \mathsf{n} \cdot (\mathsf{n}^j \cdot b \sqcap \bigsqcap_{l<j} \mathsf{n}^l \cdot a) \\ = & a \sqcap \mathsf{n} \cdot (a \boxed{j} b) \\ = & a \,\square\, (a \boxed{j} b) \ , \end{array}$$

where

$$c \,\square\, d =_{df} c \boxed{1} d = c \sqcap \mathsf{n} \cdot d \ . \tag{5}$$

The inductive clause for $\boxed{j}$ will be the basis for an inductive (or recursive) formulation of the until semantics.

With the help of our definition we can now formulate the semantics of until more compactly as

$$[\![\varphi \,\mathsf{U}\, \psi]\!] = \bigsqcup_{j \geq 0} [\![\varphi]\!] \ \boxed{j} \ [\![\psi]\!] \ . \tag{6}$$

The operator $\square$ enjoys a number of pleasant properties, as will be seen below. However, in general it is neither associative nor does it have a neutral element. Nevertheless it gives rise to an analogue of the Kleene star which will even allow us to bring the semantics of the until operator into closed form.

To do this, we abstract from the concrete definitions above.

Definition 5.1 Consider a set S and an arbitrary, possibly non-associative operator $\square : S \times S \to S$.

1. We define the iterations $\boxed{j}$ of $\square$ as above by

$$a \boxed{0} b =_{df} b, \qquad a \boxed{j+1} b =_{df} a \,\square\, (a \boxed{j} b) \ .$$

2. The structure $(S, \square)$ is called an *iteration algebra* if S is a complete lattice with order $\leq$, least element 0 and binary supremum operator $+$, and $\square$ is isotone in both arguments.
3. In an iteration algebra we define variants of the star and omega operators:

$$a \boxed{*} b =_{df} \mu f_{a,b} \text{ where } f_{a,b}(x) =_{df} a \,\square\, x + b \ , \ a^{\boxed{\omega}} =_{df} \nu x \,.\, a \,\square\, x \ . \tag{7}$$

In fact, $\boxed{*}$ corresponds to Kleene's original definition of $*$ as an infix operator in [11]. Hence $\boxed{*}$ and $^{\boxed{\omega}}$ have properties analogous to those of * and $^\omega$.

Lemma 5.2 *Consider an iteration algebra $(S, \Box)$.*

1. *The operators $\boxast$ and $\boxed{\omega}$ are isotone.*
2. $a \mathbin{\boxed{i+j}} a = a \mathbin{\boxed{i}} (a \mathbin{\boxed{j}} b)$.
3. *If $\Box$ is right-strict and distributes through arbitrary joins and binary meets in its right argument then $f_{a,b}$ from (7) is continuous and $a \boxast b = \bigsqcup_{j \geq 0} a \mathbin{\boxed{j}} b$.*
4. $b \leq a \boxast b$.
5. $a \Box b \leq a \boxast b$.
6. $a \boxast (a \Box b) \leq a \Box (a \boxast b)$.
7. $a \boxast (a \boxast b) = a \boxast b$.
8. *If $\Box$ is left-strict, i.e., if $0 \Box a = 0$ for all a, then $0 \boxast b = b$ and $0^{\boxed{\omega}} = 0$.*
9. *If $a \Box 0 = 0$ then $a \boxast 0 = 0$.*
10. *If $\Box$ is left-distributive then $a \boxast (b + c) = a \boxast b + a \boxast c$.*
11. $a \boxast a^{\boxed{\omega}} = a^{\boxed{\omega}}$.
12. *If S is a universally distributive complete lattice then* $\nu f_{a,b} = \mu f_{a,b} + a^{\boxed{\omega}} = a \boxast b + a^{\boxed{\omega}}$.

Proof.

1. Immediate from Tarski's fixed point theorem [21].
2. Straightforward induction.
3. Continuity of $f_{a,b}$ is immediate from the assumptions. Another straightforward induction shows $f^i_{a,b}(0) = \bigsqcup_{j \leq i} a \mathbin{\boxed{j}} b$ for $i \in \mathbb{N}$, from which the claim follows by lattice algebra and Kleene's fixed point theorem [10].
4. Immediate from (7).
5. Immediate from Part 4, isotony of $\Box$ and (7).
6. By least fixed point induction (15), lattice algebra, isotony of $\Box$, Part 4 and (7),

$$\begin{aligned} a \boxast (a \Box b) \leq a \Box (a \boxast b) &\Leftarrow a \Box b + a \Box (a \Box (a \boxast b)) \leq a \Box (a \boxast b) \\ &\Leftrightarrow a \Box b \leq a \Box (a \boxast b) \land a \Box (a \Box (a \boxast b)) \leq a \Box (a \boxast b) \\ &\Leftarrow b \leq a \boxast b \land a \Box (a \boxast b)) \leq a \boxast b \Leftrightarrow \mathsf{TRUE}\ . \end{aligned}$$

7. $(\geq)$ is immediate from Part 4.
   $(\leq)$ By least fixed point induction (15), lattice algebra and reflexivity of $\leq$,

$$\begin{aligned} a \boxast (a \boxast b) \leq a \boxast b &\Leftarrow a \boxast b + a \Box (a \boxast b) \leq a \boxast b \\ &\Leftarrow a \Box (a \boxast b) \leq a \boxast b \\ &\Leftarrow a \boxast b = f_{a,b}(a \boxast b)\ . \end{aligned}$$

8. Immediate from (7).
9. Immediate from (7).
10. $(\geq)$ is just isotony of $\Box$.
    $(\leq)$ By least fixed point induction (15), left distributivity of $\Box$, (7) and isotony of $+$,

$$\begin{aligned} a \boxast (b + e) \leq a \boxast b + a \boxast e &\Leftarrow b + e + a \Box (a \boxast b + a \boxast e) \leq a \boxast b + a \boxast e \\ &\Leftarrow b + e + a \Box (a \boxast b) + a \Box (a \boxast e) \leq a \boxast b + a \boxast e \Leftrightarrow \mathsf{TRUE}\ . \end{aligned}$$

11. ($\geq$) Immediate by Part 4.
    ($\leq$) By least fixed point induction (15), lattice algebra and (7),
$$a \circledast a^{\boxed{\omega}} \leq a^{\boxed{\omega}} \Leftarrow a^{\boxed{\omega}} + a \mathbin{\Box} a^{\boxed{\omega}} \leq a^{\boxed{\omega}} \Leftrightarrow \mathsf{TRUE}\ .$$
12. The proof is a straightforward application of ν-fusion (20) (see [15] for the case of $^{\omega}$).

$\Box$

A main tool used in the subsequent sections is that of projections from one iteration algebra to another.

Definition 5.3 Let $(S_i, \Box_i)_{i=1,2}$ be iteration algebras. A *homomorphism* between them is a function $h : S_1 \to S_2$ that is continuous and strict and preserves $+$ and $\Box$ in that $h(a{+}b) = h(a){+}h(b)$ and $h(a \Box_1 b) = h(a) \Box_2 h(b)$ for all $a, b \in S_1$.

Lemma 5.4 *Let $(S_i, \Box_i)_{i=1,2}$ be iteration algebras with a* homomorphism *$h : S_1 \to S_2$. Then h preserves $\circledast$ as well, i.e., $h(a \circledast_1 b) = h(a) \circledast_2 h(b)$ for all $a, b \in S_1$. If h is co-continuous and* co-strict *, i.e., satisfies $h(\top) = \top$, then it also preserves $^{\boxed{\omega}}$, i.e., $h(a^{\boxed{\omega}_1}) = h(a)^{\boxed{\omega}_2}$ for all $a \in S_1$.*

Proof. By the conditions on h this is just an application of μ-fusion (18) and ν-fusion (20). $\Box$

We now return to the concrete instance of $\Box$ defined in (5). To make use of Lm. 5.2 we need to ensure that $\Box$ has the required properties. Fortunately, this is achieved by a second requirement on the semantic element n, motivated by the semantics of X as follows. In $\mathsf{TRC}(\Sigma)$, for arbitrary formula φ and its semantics $U = [\![\varphi]\!]$ we want
$$[\![\mathsf{X}\varphi]\!] = \mathsf{n} \bowtie U = \mathsf{n} \bowtie \bigcup_{u \in U} \{u\} = \bigcup_{u \in U} \mathsf{n} \bowtie \{u\}\ .$$
Therefore, we require that in the abstract quantale semantics left multiplication by n distributes through arbitrary joins.

Definition 5.5 In a left quantale S we call $\mathsf{n} \in S$ a *step* if left multiplication by n distributes through arbitrary joins and binary meets. In particular, $\mathsf{n} \cdot 0 = 0$.

Now Lm. 5.2 applies and yields the following theorem that provides an important check of the adequacy of our definitions.

Theorem 5.6 *Assume a Boolean left quantale with a step n. Then*
$$[\![\varphi \,\mathsf{U}\, \psi]\!] = [\![\varphi]\!] \circledast [\![\psi]\!]\ .$$

Proof. First, since in every Boolean algebra one has the shunting rule $x \sqcap y \leq z \Leftrightarrow x \leq \overline{y} + z$, a Galois connection, $\sqcap$ preserves all existing joins. Since by assumption left multiplication by n distributes through arbitrary joins, the function $f_{[\![\varphi]\!],[\![\psi]\!]}$ does the same. Therefore the claim is established by (6) and Lm. 5.2.3. $\Box$

This yields the following simpler closed representation of F like in Sect. 2:

Corollary 5.7 $[\![\mathsf{F}\psi]\!] = \mathsf{n}^* \cdot [\![\psi]\!]$. *In particular,* $[\![\mathsf{F}\top]\!] = \top$.

Proof. First, by (7), (5) and Boolean algebra,

$$f_{\top,[\![\psi]\!]}(x) = (\top \sqcap \mathsf{n} \cdot x) + [\![\psi]\!] = \mathsf{n} \cdot x + [\![\psi]\!] \ .$$

Hence, by the definition of F, Th. 5.6, (3), (7) and Def. 3.1.4,

$$[\![\mathsf{F}\psi]\!] = [\![\top \,\mathsf{U}\, \psi]\!] = [\![\top]\!] \circledast [\![\psi]\!] = \top \circledast [\![\psi]\!] = \mu f_{\top,[\![\psi]\!]} = \mathsf{n}^* \cdot [\![\psi]\!] \ .$$

The operator G and its relation with the $\boxed{\omega}$ operator are treated in Sect. 7.

6 The Next-Time Operator

We now discuss the connection between (1) and (LDM) in the algebraic setting. To satisfy (1), we need to have for all formulas φ and their semantic values $a =_{df} [\![\varphi]\!]$ that $\overline{\mathsf{n} \cdot a} = [\![\neg\mathsf{X}\varphi]\!] = [\![\mathsf{X}\neg\varphi]\!] = \mathsf{n} \cdot \overline{a}$. This semantic property can equivalently be characterised as follows (Parts 1 and 2 were already shown in [3]).

Lemma 6.1 *Consider a Boolean IL-semiring* S *and* $\mathsf{n} \in S$.

1. *If* n *is left-distributive and satisfies* $\forall\, a \in S : \mathsf{n} \cdot \overline{a} \le \overline{\mathsf{n} \cdot a}$ *then* (LDM) *and* $\mathsf{n} \cdot 0 = 0$ *hold.*
2. *If* (LDM) *and* $\mathsf{n} \cdot 0 = 0$ *hold then so does* $\forall\, a \in S : \mathsf{n} \cdot \overline{a} \le \overline{\mathsf{n} \cdot a}$.
3. *If* n *is left-distributive then* $\forall\, a \in S : \overline{\mathsf{n} \cdot a} \le \mathsf{n} \cdot \overline{a} \Leftrightarrow \mathsf{n} \cdot \top = \top \Leftrightarrow \mathsf{n}^\omega = \top$.
4. *If* n *satisfies* (LDM) *and* $\forall\, a : \mathsf{n} \cdot \overline{a} = \overline{\mathsf{n} \cdot a}$ *then* n *is left-distributive.*

Proof.

1. For (LDM) it suffices to show ($\ge$), since the reverse inequality follows by isotony. By shunting, the assumption $\mathsf{n} \cdot \overline{a} \le \overline{\mathsf{n} \cdot a}$ for all a, left distributivity, Boolean algebra and lattice algebra with isotony,

$$\begin{aligned} \mathsf{n} \cdot a \sqcap \mathsf{n} \cdot b \le \mathsf{n} \cdot (a \sqcap b) &\Leftrightarrow \mathsf{n} \cdot a \le \overline{\mathsf{n} \cdot b} + \mathsf{n} \cdot (a \sqcap b) \\ &\Leftarrow \mathsf{n} \cdot a \le \mathsf{n} \cdot \overline{b} + \mathsf{n} \cdot (a \sqcap b) \Leftrightarrow \mathsf{n} \cdot a \le \mathsf{n} \cdot (\overline{b} + (a \sqcap b)) \\ &\Leftrightarrow \mathsf{n} \cdot a \le \mathsf{n} \cdot (\overline{b} + a) \Leftrightarrow \mathsf{TRUE} \ . \end{aligned}$$

   For the second claim we reason as follows. By Boolean algebra, isotony, the assumption and Boolean algebra,

$$\mathsf{n} \cdot 0 = \mathsf{n} \cdot (1 \sqcap \overline{1}) \le \mathsf{n} \cdot 1 \sqcap \mathsf{n} \cdot \overline{1} \le \mathsf{n} \cdot 1 \sqcap \overline{\mathsf{n} \cdot 1} = 0 \ .$$

2. We calculate

$$0 = \mathsf{n} \cdot 0 = \mathsf{n} \cdot (a \sqcap \overline{a}) = \mathsf{n} \cdot a \sqcap \mathsf{n} \cdot \overline{a}.$$

   Now the claim is immediate by shunting.

3. Consider an arbitrary fixed element $a \in S$. By shunting, left distributivity, Boolean algebra, greatest element and $\mathsf{n}^\omega = \nu y \,.\, \mathsf{n} \cdot y$,

$$\overline{\mathsf{n} \cdot a} \le \mathsf{n} \cdot \overline{a} \Leftrightarrow \top \le \mathsf{n} \cdot a + \mathsf{n} \cdot \overline{a} \Leftrightarrow \top \le \mathsf{n} \cdot (a + \overline{a}) \\ \Leftrightarrow \top \le \mathsf{n} \cdot \top \Leftrightarrow \top = \mathsf{n} \cdot \top \Leftrightarrow \mathsf{n}^\omega = \top .$$

4. By De Morgan, the assumption, (LDM), the assumption twice and Boolean algebra,

$$\mathsf{n} \cdot (a + b) = \mathsf{n} \cdot \overline{(\overline{a} \sqcap \overline{b})} = \overline{\mathsf{n} \cdot (\overline{a} \sqcap \overline{b})} = \overline{\mathsf{n} \cdot \overline{a} \sqcap \mathsf{n} \cdot \overline{b}} = \overline{\overline{\mathsf{n} \cdot a} \sqcap \overline{\mathsf{n} \cdot b}} = \mathsf{n} \cdot a + \mathsf{n} \cdot b \ .$$

□

In relation algebra, the special case $\mathsf{n} \cdot \overline{1} \le \overline{\mathsf{n}}$ of the property in Part 1 characterises n as a partial function and is equivalent to the full property $\forall\, a : \mathsf{n} \cdot \overline{a} \le \overline{\mathsf{n} \cdot a}$ [20]. But in general quantales the special and the full case are not equivalent [3]. Moreover, again from [3], we know that in quantales such as WOR and TRC left multiplication by an element n distributes over meet iff n is prefix-free, i.e., if no member of n is a prefix of another member. This holds in particular if all traces in n have equal length, which is the case if n models a transition relation and hence consists only of traces of length 2. The equivalent condition $\forall\, a : \mathsf{n} \cdot a \sqcap \mathsf{n} \cdot \overline{a} = 0$ was used in the computation calculus of R.M. Dijkstra [6].

But what about Part 3 of Lm. 6.1? Only rarely will a quantale be "generated" by n in the sense that $\mathsf{n}^\omega = \top$. We deal with this problem in Sects. 7 and 8.

7 Infinitary Semantics of CTL*

Before we tackle a general algebraic solution to the problem mentioned at the end of the previous section, let us look at the concrete quantale $S = \mathsf{TRC}(\Sigma)$. There we definitely do *not* have $\mathsf{n}^\omega = \top$ for $\mathsf{n} = \Sigma.\Sigma$, since $\mathsf{n}^\omega = \Sigma^\omega = \mathsf{inf}\, S$, where the inf operator was introduced in Ex. 3.2.

We will show that restricting the semantics given in Sect. 4 to infinite traces remedies the problem, while at the same time faithfully reflecting the original semantics of CTL^*, which was given in terms of infinite sequences of states anyway.

To obtain an abstract algebraic version of this, we need some additional notions. The key is the observation in Ex. 3.2 that $U \bowtie \emptyset = \mathsf{inf}\, U$ and hence $U \bowtie \emptyset = \emptyset$ iff $\mathsf{inf}\, U = \emptyset$. This motivates the following definition.

Definition 7.1 Assume a bounded IL-semiring S.

1. The *purely infinite part* of $a \in S$ is $\mathsf{inf}\, a =_{df} a \cdot 0$. We set $\mathsf{N} =_{df} \mathsf{inf}\, \top$. We call *a purely infinite* if $a = \mathsf{inf}\, a$. The set of all purely infinite elements is denoted by $\mathsf{infel}(S)$.
2. Dually, we call *a purely finite* if $\mathsf{inf}\, a = a \cdot 0 \le 0$, i.e., if its purely infinite part is trivial. The right hand side is equivalent to $a \cdot 0 = 0$.

3. If S is Boolean we can define the *purely finite part* of $a \in S$ analogously as in $\mathsf{TRC}(\Sigma)$ by $\mathsf{fin}\, a =_{df} a - \mathsf{inf}\, a$.

We state some simple consequences of the definition; for more details see [15].

Lemma 7.2 *Consider arbitrary $a, b \in S$.*

1. *If b is purely infinite then so is $a \cdot b$.*
2. $\mathsf{inf}\,(a \cdot b) = a \cdot \mathsf{inf}\, b$. *In particular,* inf *commutes with left restriction, i.e., for* $p \in \mathsf{test}(S)$, $\mathsf{inf}\,(p \cdot b) = p \cdot \mathsf{inf}\, b$.
3. $a \cdot \mathsf{N} \leq \mathsf{N}$.
4. *The operator* inf *is a kernel operator, i.e., it is contractive* ($\mathsf{inf}\, a \leq a$)*, isotone and idempotent* ($\mathsf{inf}\,(\mathsf{inf}\, a) = \mathsf{inf}\, a$)*. By the latter fact the functionality of the operator can be made precise as* $\mathsf{inf} : S \to \mathsf{infel}(S)$.

Proof.

1. By associativity and assumption, $(a \cdot b) \cdot 0 = a \cdot (b \cdot 0) = a \cdot b$.
2. By the definitions and associativity,
$$\mathsf{inf}\,(a \cdot b) = (a \cdot b) \cdot 0 = a \cdot (b \cdot 0) = a \cdot \mathsf{inf}\, b \ .$$
3. By the definition of N, greatestness of $\top$ with isotony of $\cdot$ and the definition of N again,
$$a \cdot \mathsf{N} = a \cdot \top \cdot 0 \leq \top \cdot 0 = \mathsf{N} \ .$$
4. For contractivity, we have by definition, leastness of 0 with isotony of $\cdot$ and neutrality of 1 that $\mathsf{inf}\, a = a \cdot 0 \leq a \cdot 1 = a$.
Isotony is immediate from the definition and isotony of $\cdot$.
For idempotence, by the definition, associativity, annihilation and the definition again,
$$\mathsf{inf}\,(\mathsf{inf}\, a) = (a \cdot 0) \cdot 0 = a \cdot (0 \cdot 0) = a \cdot 0 = \mathsf{inf}\, a \ .$$
□

In general IL-semirings we cannot give a closed expression for the operator fin. However, in left Kleene algebras we can show closedness of the purely finite elements under star.

Lemma 7.3 *If $a \cdot 0 = 0$ then also $a^* \cdot 0 = 0$.*

By least fixed point induction for star (using Def. 3.1.4) and lattice algebra,

$$a^* \cdot 0 \leq 0 \ \Leftarrow\ 0 + a \cdot 0 \leq 0 \ \Leftrightarrow\ a \cdot 0 \leq 0 \ .$$

We show a few properties of the inf operator.

Lemma 7.4 *Assume a Boolean IL-semiring S.*

1. $\mathsf{inf}\, a = \mathsf{N} \sqcap a$ *and* $\mathsf{inf}\, \overline{a} = \mathsf{N} - a = \mathsf{N} - \mathsf{inf}\, a$.

2. *Element a is purely infinite iff $a \le \mathsf{N}$. Hence $\mathsf{infel}(S)$ is downward closed.*

Let now S be a Boolean left quantale.

3. *The set $\mathsf{infel}(S)$ forms a complete lattice with greatest element N in which suprema of arbitrary and and infima of non-empty subsets coincide with the ones in S. For the empty subset we have $\bigsqcap \emptyset = \mathsf{N}$.*
   $\mathsf{inf} : S \to \mathsf{infel}(S)$ *is universally disjunctive and conjunctive.*

Proof.

1. Repeatedly using the definition of N and inf, Boolean algebra, isotony and neutrality of 1,

$$\begin{aligned} a \sqcap \mathsf{N} &= a \sqcap \top \cdot 0 = a \sqcap (\overline{a} + a) \cdot 0 = a \sqcap (\overline{a} \cdot 0 + a \cdot 0) \le \sqcap (\overline{a} \cdot 1 + a \cdot 0) \\ &= a \sqcap (\overline{a} + a \cdot 0) = a \cdot 0 = \mathsf{inf}\, a = a \cdot 0 \le a \cdot 1 \sqcap \top \cdot 0 = a \sqcap \mathsf{N} \ . \end{aligned}$$

   Moreover, by the just proved representation and Boolean algebra,

$$\neg_i \, \mathsf{inf}\, a = \mathsf{N} \sqcap \overline{(\mathsf{N} \sqcap a)} = \mathsf{N} \sqcap (\overline{\mathsf{N}} + \overline{a}) = \mathsf{N} \sqcap \overline{a} = \neg_i \, a \ .$$

2. Using lattice algebra and Part 1 we have $a \le \mathsf{N} \Leftrightarrow a = a \sqcap \mathsf{N} \Leftrightarrow a = \mathsf{inf}\, a$.
3. By definition the purely infinite elements are precisely the fixed points of the isotone function $\lambda x \,.\, x \cdot 0$; hence by Tarski's generalised fixed point theorem [21] they form a complete lattice by themselves. Greatestness of N follows from Part 2; it also entails the claim $\bigsqcap \emptyset = \mathsf{N}$. For an arbitrary subset $T \subseteq \mathsf{infel}(S)$, by Part 2 all elements of T are $\le \mathsf{N}$; hence, by lattice algebra, so is their supremum $\bigsqcup T$ which thus, again by Part 2, lies in $\mathsf{infel}(S)$ as well. Assume now that T is non-empty. Then, by the downward closure of $\mathsf{infel}(S)$ stated in Part 2, any lower bound of T and, in particular, $\bigsqcap T$ lies in $\mathsf{infel}(S)$ as well.
   Consider an arbitrary subset $T \subseteq S$. By Part 1, complete distributivity of complete Boolean algebras (see the beginning of the proof of Th. 5.6) and Part 1 again we have

$$\mathsf{inf}\,(\bigsqcup T) = N \sqcap \bigsqcup T = \bigsqcup \{N \sqcap a \,|\, a \in T\} = \bigsqcup \{\mathsf{inf}\, a \,|\, a \in T\} \ .$$

   Assume now that T is non-empty. By Part 1, lattice algebra and Part 1 again we have

$$\mathsf{inf}\,(\bigsqcap T) = N \sqcap \bigsqcap T = \bigsqcap \{N \sqcap a \,|\, a \in T\} = \bigsqcap \{\mathsf{inf}\, a \,|\, a \in T\} \ .$$

   All this implies universal disjunctivity and conjunctivity of inf. □

Now we can give our modified semantics for CTL^*.

Definition 7.5 The *infinitary semantics* $[\![\varphi]\!]_i$ of a CTL^* formula φ over a Boolean left quantale is defined as follows:

- $[\![\mathsf{E}\varphi]\!]_i =_{df} \ulcorner[\![\varphi]\!]_i \cdot \mathsf{N}$.
- For all other formulas φ we set $[\![\varphi]\!]_i =_{df} \mathsf{inf}\,[\![\varphi]\!]$.

As an auxiliary we define complementation relative to N as

$$\neg_i\, a =_{df} \mathsf{N} - a \; . \tag{8}$$

This satisfies the following properties.

Theorem 7.6 *Assume a Boolean left quantale S with a step n.*

1. *The pair $(\mathsf{infel}(S), \Box_i)$ where $\Box_i$ is the restriction of $\Box$ to $\mathsf{infel}(S)$ is an iteration algebra and inf is a homomorphism from $(S, \Box)$ to $(\mathsf{infel}(S), \Box_i)$.*
2. *$[\![\neg\varphi]\!]_i = \neg_i\,[\![\varphi]\!]_i$ and $\neg_i\,\neg_i\, a = \mathsf{inf}\, a$.*
3. *The semantics $[\![\,]\!]_i$ propagates inductively:*

$$[\![\bot]\!]_i = 0 \; , \qquad [\![\mathsf{X}\,\varphi]\!]_i = \mathsf{n} \cdot [\![\varphi]\!]_i \; ,$$
$$[\![p]\!]_i = p \cdot \mathsf{N} \; , \qquad [\![\varphi\,\mathsf{U}\,\psi]\!]_i = [\![\varphi]\!]_i \boxast_i [\![\psi]\!]_i \; ,$$
$$[\![\varphi \to \psi]\!]_i = \neg_i\,[\![\varphi]\!]_i + [\![\psi]\!]_i \; .$$

   In addition,

$$[\![\varphi \vee \psi]\!]_i = [\![\varphi]\!]_i + [\![\psi]\!]_i \; , \; [\![\varphi \wedge \psi]\!]_i = [\![\varphi]\!]_i \sqcap [\![\psi]\!]_i \; , \; [\![\mathsf{A}\varphi]\!]_i = \neg\ulcorner(\neg_i\,[\![\varphi]\!]_i) \cdot \mathsf{N} \; .$$

4. *If $\mathsf{N} \leq \mathsf{n} \cdot \mathsf{N}$ (and hence $\mathsf{N} \leq \mathsf{n}^\omega$) then for all $a \in S$ we have $\mathsf{inf}\,(\mathsf{n} \cdot \overline{a}) = \mathsf{inf}\,\overline{\mathsf{n} \cdot a}$. In particular, $[\![\mathsf{X}\,\neg\varphi]\!]_i = [\![\neg\mathsf{X}\,\varphi]\!]_i$. Furthermore, for all $a \in S$ we have $\neg_i\,(\mathsf{n} \cdot \mathsf{inf}\,\overline{a}) = \mathsf{n} \cdot \mathsf{inf}\, a$.*
5. *If $\mathsf{N} \leq \mathsf{n} \cdot \mathsf{N}$ then $[\![\mathsf{F}\psi]\!]_i = \mathsf{n}^* \cdot [\![\psi]\!]_i$ and $[\![\mathsf{G}\psi]\!]_i = [\![\psi]\!]_i^{\boxed{\omega}_i}$.*

Proof.

1. By Lm. 7.4.3 $\mathsf{infel}(S)$ is a complete lattice. Isotony of $\Box_i$ is immediate from its definition and isotony of $\sqcap$ and $\cdot$. By Lm. 7.4.3 inf is continuous and strict. Finally by Lm. 7.4.3 and Lm. 7.2.2,

$$\mathsf{inf}\,(a \,\Box\, b) = \mathsf{inf}\,(a \sqcap \mathsf{n} \cdot b) = \mathsf{inf}\, a \sqcap \mathsf{inf}\,(\mathsf{n} \cdot b) = \mathsf{inf}\, a \sqcap \mathsf{n} \cdot \mathsf{inf}\, b = \mathsf{inf}\, a \,\Box_i\, \mathsf{inf}\, b \; .$$

2. The first claim is immediate from (3) and Lm. 7.4.1. For the second one we have by (8), Boolean algebra and Lm. 7.4.1

$$\neg_i\,\neg_i\, a = \mathsf{N} - (\mathsf{N} - a)) = \mathsf{N} \sqcap a = \mathsf{inf}\, a \; .$$

3. Recall Def. 4.1. The first property is immediate from Def. 7.5, while the second one is an instance of Lm. 7.2.2.
   The third property follows from Lm. 7.4.3 and Lm. 7.4.1.
   The fourth property is again an instance of Lm. 7.2.2.
   The fifth property is straightforward from Part 1 and Lm. 5.4.
   The additional equations are immediate from Lm. 7.4.1.

4. From Lm. 6.1.2 we know $\mathsf{n} \cdot \overline{a} \le \overline{\mathsf{n} \cdot a}$, and isotony of inf (Lm. 7.2.4) shows $\mathsf{inf}\,(\mathsf{n} \cdot \overline{a}) \le \mathsf{inf}\,\overline{\mathsf{n} \cdot a}$. For the converse inequation we reason as follows.

   By Lm. 7.4.1, Lm. 7.2.2, shunting, additivity of inf and left distributivity of n, Boolean algebra with the definition of N and the assumption,

$$\begin{aligned} \mathsf{inf}\,\overline{\mathsf{n} \cdot a} \le \mathsf{inf}\,(\mathsf{n} \cdot \overline{a}) &\Leftrightarrow \mathsf{N} \sqcap \overline{\mathsf{inf}\,(\mathsf{n} \cdot a)} \le \mathsf{inf}\,(\mathsf{n} \cdot \overline{a}) \\ &\Leftrightarrow \mathsf{N} \sqcap \overline{\mathsf{n} \cdot \mathsf{inf}\,a} \le \mathsf{inf}\,(\mathsf{n} \cdot \overline{a}) \\ &\Leftrightarrow \mathsf{N} \le \mathsf{n} \cdot \mathsf{inf}\,a + \mathsf{n} \cdot \mathsf{inf}\,\overline{a} \Leftrightarrow \mathsf{N} \le \mathsf{n} \cdot \mathsf{inf}\,(a + \overline{a}) \\ &\Leftrightarrow \mathsf{N} \le \mathsf{n} \cdot \mathsf{N} \Leftrightarrow \mathsf{TRUE}\ . \end{aligned}$$

   For the final claim we calculate, by Lm. 7.2.2, the first claim of this part, Lm. 7.4.1, Boolean algebra, Lm. 7.4.1 and Lm. 7.2.2,

$$\begin{aligned} \neg_i\,(\mathsf{n} \cdot \mathsf{inf}\,\overline{a}) &= \neg_i\,\mathsf{inf}\,(\mathsf{n} \cdot \overline{a}) = \neg_i\,\mathsf{inf}\,\overline{\mathsf{n} \cdot a} = \neg_i\,(\neg_i\,\mathsf{n} \cdot a) \\ &= \mathsf{N} \sqcap \mathsf{n} \cdot a = \mathsf{inf}\,(\mathsf{n} \cdot a) = \mathsf{n} \cdot \mathsf{inf}\,a\ . \end{aligned}$$

5. The proof of the equation for F
   follows closely the one for Cor. 5.7. By (7) the generating function for $a \circledast_i b$ is $f_{a,b}(x) =_{df} a \,\Box_i\, x + b$. We obtain by (5), Parts 1 and 2 of Lm. 7.2 and Boolean algebra,

$$f_{\mathsf{N},[\![\psi]\!]_i}(x) = \mathsf{N} \,\Box_i\, x + [\![\psi]\!]_i = (\mathsf{N} \sqcap \mathsf{n} \cdot x) + [\![\psi]\!]_i = \mathsf{n} \cdot x + [\![\psi]\!]_i\ .$$

   Hence, by the definition of F, Th. 5.6, (3), (7) and Def. 3.1.4,

$$[\![\mathsf{F}\psi]\!]_i = [\![\top\,\mathsf{U}\,\psi]\!]_i = [\![\top]\!] \circledast_i [\![\psi]\!] = \top \circledast_i [\![\psi]\!] = \mu f_{\mathsf{N},[\![\psi]\!]_i} = \mathsf{n}^* \cdot [\![\psi]\!]\ .$$

   We now turn to the equation for G.
   For that we recall from Def. 13.3 the De Morgan dual $f^\circ(y) =_{df} \overline{f(\overline{y})}$ of a function $f : S \to S$ over a Boolean algebra S and the property from Lm. 13.4 that $\mu f = \overline{\nu f^\circ}$ and $\nu f = \overline{\mu f^\circ}$. By the definition of G, Lm. 13.4 and the above representation of F therefore

$$[\![\mathsf{G}\psi]\!]_i = \neg_i\,[\![\mathsf{F}\neg\psi]\!]_i = \neg_i\,\mu f_{\neg\psi} = \nu f^\circ_{\neg\psi}\ .$$

   By definition of duals, definition of $f_{\neg\psi}$, Boolean algebra, Parts 2 and 4, Part 2 again $[\![\psi]\!]_i, y \in \mathsf{infel}(S)$ and the definition of $\Box$,

$$\begin{aligned} f^\circ_{\neg\psi}(y) &= \neg_i\, f_{\neg\psi}(\neg_i\, y) = \neg_i\,([\![\neg\psi]\!]_i + \mathsf{n} \cdot (\neg_i\, y)) \\ &= (\neg_i\,[\![\neg\psi]\!]_i) \sqcap (\neg_i\,(\mathsf{n} \cdot (\neg_i\, y))) \\ &= (\neg_i\,(\neg_i\,[\![\psi]\!]_i)) \sqcap \mathsf{n} \cdot \mathsf{inf}\,y = (\mathsf{N} \sqcap [\![\psi]\!]_i) \sqcap \mathsf{n} \cdot y = [\![\psi]\!]_i \,\Box_i\, y\ . \end{aligned}$$

   Now the claim follows from (7). □

□

This means that we have now obtained a semantics which faithfully mirrors the original CTL^* semantics.

We combine the results of this theorem with our results on the until operator.

Corollary 7.7 *Assume again* $\mathsf{N} \le \mathsf{n} \cdot \mathsf{N}$ *and define, for formulas* φ *and* ψ *the abbreviation* $\varphi \mathsf{W} \psi \ \Leftrightarrow_{df} \ \mathsf{G}\varphi \vee (\varphi \mathsf{U} \psi)$*. Then* $[\![\varphi \mathsf{W} \psi]\!]_i = \nu y \,.\, [\![\psi]\!]_i + ([\![\varphi]\!]_i \,\Box_i\, y)$.

Proof. This follows from Lm. 5.2.12 together with Ths. 7.6.3 and 7.6.5. $\square$

In the literature the operator W is known as *weak until* or *while*. It expresses that φ holds forever or else ψ will eventually hold forever with φ holding all the time before that.

8 Generated Quantales

In view of Th. 7.6.4 we introduce a new notion.

Definition 8.1 Assume a Boolean quantale S with a step $\mathsf{n} \in S$. Then S is called n-*generated* if $\top = \nu x \,.\, 1 + \mathsf{n} \cdot x = \mathsf{n}^* + \mathsf{n}^\omega$ and $\mathsf{n}^\omega \le \mathsf{N}$. If additionally $\ulcorner \mathsf{N} = 1$ then S is *strongly* n-*generated*.

The definition means that all elements of S can be obtained by finite or infinite iteration of n. The constraint $\mathsf{n}^\omega \le \mathsf{N}$ serves to exclude "pseudo-infinite" iterations of n. Strong generation means that all starting states can be extended into infinite computations.

Example 8.2 The quantale $\mathsf{TRC}(\Sigma)$ (Ex. 3.2) is strongly $\Sigma.\Sigma$-generated, while its reduct to finite traces is not. $\square$

The definition of generatedness has important structural consequences. For any IL-Semiring let

$$\mathsf{rtest}(S) \ =_{df} \ \{p \cdot \mathsf{N} \mid p \in \mathsf{test}(S)\} \tag{9}$$

be the set of *relative test ideals* of S; each of them characterises the set of infinite traces with starting states in a state set p.

Lemma 8.3 *Consider an* n-*generated quantale* S.

1. $\mathsf{N} = \mathsf{n}^\omega$ *and* $\mathsf{N} \sqcap \mathsf{n}^* = 0$*. Hence* n^ω *and* n^* *are complements of each other.*
2. $\mathsf{N} = \mathsf{n} \cdot \mathsf{N}$.
3. $\mathsf{n}^\omega = \mathsf{inf}\,(\mathsf{n}^\omega)$ *and hence* $\mathsf{n}^\omega \cdot \mathsf{n}^\omega = \mathsf{n}^\omega = (\mathsf{n}^\omega)^\omega$.

Consider now the concrete operator $c \,\Box\, d \ =_{df} \ c \sqcap \mathsf{n} \cdot d$ *from* (5).

4. *For all* $a \in S$ *we have* $a^{\boxed{\omega}} \le \mathsf{N}$.
5. $\mathsf{n}^{\boxed{\omega}} = 0$.
6. *If* $a \in S$ *is purely infinite then* $a^{\boxed{\omega}} = \bigsqcap_{k \in \mathbb{N}} \mathsf{n}^k \cdot a$.

Assume now that S *is strongly* n-*generated.*

7. $\ulcorner \mathsf{n} = 1$.
8. *The sets* $\mathsf{test}(S)$ *and* $\mathsf{rtest}(S)$ *are order-isomorphic.*

Proof.

1. By definition of N, generatedness and right distributivity, $\mathsf{n}^* \cdot 0 = 0$ (Lm. 7.3) with neutrality of 0 and $0 \leq 1$ with isotony,

$$\mathsf{N} = \top \cdot 0 = \mathsf{n}^* \cdot 0 + \mathsf{n}^\omega \cdot 0 = \mathsf{n}^\omega \cdot 0 \leq \mathsf{n}^\omega \ .$$

Now the first claim follows by the assumption $\mathsf{n}^\omega \leq \mathsf{N}$ and antisymmetry. For the second claim we show that 0 is the only lower bound of N and n^*. By isotony, Lms. 7.4.2 and 7.3, and transitivity,

$$a \leq \mathsf{N} \wedge a \leq \mathsf{n}^* \Rightarrow a \leq \mathsf{N} \wedge a \cdot 0 \leq \mathsf{n}^* \cdot 0 \Leftrightarrow a = a \cdot 0 \wedge a \cdot 0 \leq 0 \Rightarrow a \leq 0 \ .$$

2. By Part 1 and omega unfold $\mathsf{N} = \mathsf{n}^\omega = \mathsf{n} \cdot \mathsf{n}^\omega = \mathsf{n} \cdot \mathsf{N}$.
3. By Part 1, the definition of N and idempotence of inf,

$$\mathsf{inf}\,(\mathsf{n}^\omega) = \mathsf{inf}\,\mathsf{N} = \mathsf{inf}\,(\mathsf{inf}\,\top) = \mathsf{inf}\,\top = \mathsf{N} = \mathsf{n}^\omega \ .$$

Hence, as mentioned in Def. 7.1.1, n^ω is a left zero and therefore $\mathsf{n}^\omega \cdot \mathsf{n}^\omega = \mathsf{n}^\omega$. Moreover, using omega unfold,

$$(\mathsf{n}^\omega)^\omega = \mathsf{n}^\omega \cdot (\mathsf{n}^\omega)^\omega = \mathsf{n}^\omega \ .$$

4. By definition of $^{\boxed{\omega}}$, definition of $\Box$ and lattice algebra,

$$a^{\boxed{\omega}} = a \,\Box\, a^{\boxed{\omega}} = a \sqcap \mathsf{n} \cdot a^{\boxed{\omega}} = \mathsf{n} \cdot a^{\boxed{\omega}} \ .$$

Now greatest fixed point co-induction for ω (Def.Def. 3.1.4 and (16)) and Part 1 show $a^{\boxed{\omega}} \leq \mathsf{n}^\omega = \mathsf{N}$.
5. By definition of $^{\boxed{\omega}}$, definition of $\Box$, Part 4, $\mathsf{N} = \mathsf{inf}\,\top$, Lm. 7.2.2, isotony of inf, Lm. 7.4.1 and assumption on n,

$$\mathsf{n}^{\boxed{\omega}} = \mathsf{n} \,\Box\, \mathsf{n}^{\boxed{\omega}} = \mathsf{n} \sqcap \mathsf{n} \cdot \mathsf{n}^{\boxed{\omega}} \leq \mathsf{n} \sqcap \mathsf{n} \cdot \mathsf{N} \leq \mathsf{n} \sqcap \mathsf{inf}\,(\mathsf{n} \cdot \top) \leq \mathsf{n} \sqcap \mathsf{N} = \mathsf{n} \cdot 0 = 0 \ .$$

6. First we show that the generating function $f(y) = a \,\Box_i\, y$ for $a^{\boxed{\omega}_i}$ over $\mathsf{infel}(S)$ is positively conjunctive and hence co-continuous. As a preparation we show the same for $g(y) =_{df} \mathsf{n} \cdot y$. Throughout we assume that the index set for the ks is non-empty. Using $a_k \in \mathsf{infel}(S)$ for all k with Lm. 7.4.3 and Lm. 7.2.2, De Morgan, Part 2 and Th. 7.6.4, left distributivity of n, De Morgan, Lm. 7.4.3, Part 2 and Th. 7.6.4, Boolean algebra and Lm. 7.2.2 with all $a_i \in \mathsf{infel}(S)$,

$$\begin{aligned} g(\textstyle\bigsqcap_k a_k) &= \mathsf{n} \cdot \textstyle\bigsqcap_k a_k = \mathsf{inf}\,(\mathsf{n} \cdot \textstyle\bigsqcap_k a_k) = \mathsf{inf}\,(\mathsf{n} \cdot \overline{\textstyle\bigsqcup_k \overline{a_k}}) = \mathsf{inf}\,(\overline{\mathsf{n} \cdot \textstyle\bigsqcup_k \overline{a_k}}) \\ &= \mathsf{inf}\,(\overline{\textstyle\bigsqcup_k \mathsf{n} \cdot \overline{a_k}}) = \mathsf{inf}\,(\textstyle\bigsqcap_k \overline{\mathsf{n} \cdot \overline{a_k}}) = \textstyle\bigsqcap_k \mathsf{inf}\,(\overline{\mathsf{n} \cdot \overline{a_k}}) \\ &= \textstyle\bigsqcap_k \mathsf{inf}\,(\mathsf{n} \cdot \overline{\overline{a_k}}) = \textstyle\bigsqcap_k \mathsf{inf}\,(\mathsf{n} \cdot a_k) = \textstyle\bigsqcap_k \mathsf{n} \cdot a_k = \textstyle\bigsqcap_k g(a_k) \ . \end{aligned}$$

Now, by the definition of $\square$, the equation for g just shown, lattice algebra and the definition of $\square$ again,

$$a \,\square \bigsqcap_k b_k = a \sqcap \mathsf{n}\cdot \bigsqcap_k b_k = a \sqcap (\bigsqcap_k \mathsf{n}\cdot b_k) = \bigsqcap_k (a \sqcap \mathsf{n}\cdot b_k) = \bigsqcap_k a \,\square\, b_k \ .$$

Hence, by Th. 13.5 we have $a^{\boxed{\omega}} = \nu f = \bigsqcap_k f^k(\mathsf{N})$, where $f^k(\mathsf{N}) = a \boxed{k}\, \mathsf{N}$.

By (4) we have $a \boxed{k}\, \mathsf{N} = (\bigsqcap_{j<k} \mathsf{n}^j \cdot a) \sqcap \mathsf{n}^k \cdot \mathsf{N}$. By Part 1 and the fixed point property of n^ω,

$$\mathsf{n}^k \cdot \mathsf{N} = \mathsf{n}^k \cdot \mathsf{n}^\omega = \mathsf{n}^\omega = \mathsf{N} \ .$$

Hence, by the above calculation, Lm. 7.4.1, Lm. 7.4.3, Lm. 7.2.1, and the assumption that $a \in \mathsf{infel}(S)$,

$$\begin{aligned} a \boxed{k}\, \mathsf{N} &= (\bigsqcap_{j<k} \mathsf{n}^j \cdot a) \sqcap \mathsf{n}^k \cdot \mathsf{N} = (\bigsqcap_{j<k} \mathsf{n}^j \cdot a) \sqcap \mathsf{N} = \ \mathsf{inf}\,(\bigsqcap_{j<k} \mathsf{n}^j \cdot a) \\ &= \bigsqcap_{j<k} \mathsf{inf}\,(\mathsf{n}^j \cdot a) = \bigsqcap_{j<k} \mathsf{n}^j \cdot \mathsf{inf}\, a = \bigsqcap_{j<k} \mathsf{n}^j \cdot a \ . \end{aligned}$$

Now the claim follows by straightforward lattice algebra.

7. By strong generatedness, Part 1, omega unfold, locality (Lm. 3.5.5), strong generatedness again and neutrality of 1,

$$1 = \ulcorner\mathsf{N} = \ulcorner(\mathsf{n}^\omega) = \ulcorner(\mathsf{n}\cdot\mathsf{n}^\omega) = \ulcorner(\mathsf{n}\cdot\ulcorner(\mathsf{n}^\omega)) = \ulcorner(\mathsf{n}\cdot 1) = \ulcorner\mathsf{n} \ .$$

8. We have to show, for $p, q \in \mathsf{test}(S)$,

$$p \le q \ \Leftrightarrow\ p\cdot\mathsf{N} \le q\cdot\mathsf{N} \ .$$

($\Rightarrow$) follows by isotony of $\cdot$.
($\Leftarrow$) First, for arbitrary $r \in \mathsf{test}(S)$, by locality (Lemma 3.5.5), strong generatedness with neutrality of 1 and Lemma 3.5.4,

$$\ulcorner(r\cdot\mathsf{N}) = \ulcorner(r\cdot\ulcorner\mathsf{N}) = \ulcorner r = r \ .$$

Now the claim is immediate from isotony of domain.

□

We can extend Th. 7.6.5 a bit further. Together with Lm. 8.3.6 we obtain $[\![\mathsf{G}\psi]\!]_i = \bigsqcap_{i\in\mathbb{N}} \mathsf{n}^i \cdot [\![\psi]\!]_i$. Hence, in a $*$-continuous quantale [12], i.e., a quantale with $a\cdot b^*\cdot c = \bigsqcup\{a\cdot b^n\cdot c \mid n\in\mathbb{N}\}$ for all a, b, c, we therefore have the pleasantly symmetric formulations $[\![\mathsf{F}\psi]\!]_i = \bigsqcup_{i\in\mathbb{N}} \mathsf{n}^i\cdot[\![\psi]\!]_i$ and $[\![\mathsf{G}\psi]\!]_i = \bigsqcap_{i\in\mathbb{N}} \mathsf{n}^i\cdot[\![\psi]\!]_i$.

9 Towards CTL: The Semantics of State Formulas

In this section we show, among other properties, that the semantics of each state formula has the special form of a test ideal and hence directly corresponds to a test, i.e., an abstract representation of a set of states. This will be the key to the simplified CTL semantics in Sect. 10. Throughout this section we assume an n-generated quantale.

Theorem 9.1 *Let φ be a state formula of CTL^*.*

1. *$\llbracket\varphi\rrbracket$ is a test ideal, and hence, by Lm. 3.5.4, $\llbracket\varphi\rrbracket = \ulcorner\llbracket\varphi\rrbracket \cdot \top$.*
2. *$\llbracket\varphi\rrbracket_i$ is a relative test ideal, i.e, $\llbracket\varphi\rrbracket_i = \ulcorner\llbracket\varphi\rrbracket \cdot \mathsf{N}$.*
3. *$\llbracket\mathsf{E}\varphi\rrbracket = \llbracket\varphi\rrbracket$.*
4. *$\llbracket\mathsf{A}\varphi\rrbracket = \llbracket\varphi\rrbracket$.*

Proof.

1. The proof is by induction on the structure of φ.
   - For $\bot$ and $p \in \mathsf{test}(S)$ this is immediate from Def. 4.1.
   - Assume that the claim already holds for state formulas φ and ψ. We calculate, using Def. 4.1, the induction hypothesis, Lm. 3.5.8, right distributivity and Def. 3.3,

     $$\begin{aligned}\llbracket\varphi \to \psi\rrbracket &= \overline{\llbracket\varphi\rrbracket} + \llbracket\psi\rrbracket = \overline{\ulcorner\llbracket\varphi\rrbracket \cdot \top} + \ulcorner\llbracket\psi\rrbracket \cdot \top = \neg\ulcorner\llbracket\varphi\rrbracket \cdot \top + \ulcorner\llbracket\psi\rrbracket \cdot \top \\ &= (\neg\ulcorner\llbracket\varphi\rrbracket + \ulcorner\llbracket\psi\rrbracket) \cdot \top = (\ulcorner\llbracket\varphi\rrbracket \to \ulcorner\llbracket\psi\rrbracket) \cdot \top\end{aligned}$$

     and hence by Lm. 3.5.4,

     $$\ulcorner\llbracket\varphi \to \psi\rrbracket \cdot \top = \ulcorner((\ulcorner\llbracket\varphi\rrbracket \to \ulcorner\llbracket\psi\rrbracket) \cdot \top) \cdot \top = (\ulcorner\llbracket\varphi\rrbracket \to \ulcorner\llbracket\psi\rrbracket) \cdot \top = \llbracket\varphi \to \psi\rrbracket\ .$$

   - For $\mathsf{E}\varphi$ the claim is immediate from the definition.
2. Immediate from Part 1, Def. 7.5 and Lm. 7.2.2.
3. Immediate from Part 1 and the definition of $\llbracket\mathsf{E}\varphi\rrbracket$.
4. Set for abbreviation $p =_{df} \ulcorner\llbracket\varphi\rrbracket$. Then by Part 1 we have $\llbracket\varphi\rrbracket = p \cdot \top$. Now, by Cor. 4.2, Lm. 3.5.8, Lm. 3.5.4 and Boolean algebra,

   $$\begin{aligned}\llbracket\mathsf{A}\varphi\rrbracket &= \neg\ulcorner\overline{\llbracket\varphi\rrbracket} \cdot \top = \neg\ulcorner\overline{p \cdot \top} \cdot \top \\ &= \neg\ulcorner(\neg p \cdot \top) \cdot \top = \neg\neg p \cdot \top = p \cdot \top = \llbracket\varphi\rrbracket\ .\end{aligned}$$

□

Parts 3 and 4 show that state formulas are closed under E and A. In addition we have the following result.

Lemma 9.2 *State formulas are closed under $\neg$, $\wedge$ and $\vee$.*

Proof. Let φ, ψ be state formulas with $\llbracket\varphi\rrbracket = p \cdot \top$ and $\llbracket\psi\rrbracket = q \cdot \top$. It suffices to show that the semantics $\llbracket\neg\psi\rrbracket, \llbracket\varphi \wedge \psi\rrbracket$ and $\llbracket\varphi \vee \psi\rrbracket$ each are test ideals.

- $\llbracket\neg\varphi\rrbracket = \overline{\llbracket\varphi\rrbracket} = \overline{p \cdot \top} = \neg p \cdot \top$.
- $\llbracket\varphi \wedge \psi\rrbracket = \llbracket\varphi\rrbracket \sqcap \llbracket\psi\rrbracket = p \cdot \top \sqcap q \cdot \top = p \cdot q \cdot \top$ by Lm. 3.5.7.
- $\llbracket\varphi \vee \psi\rrbracket = \llbracket\varphi\rrbracket + \llbracket\psi\rrbracket = p \cdot \top + q \cdot \top = (p + q) \cdot \top$.

□

Next, we state some properties of U and its relatives for state formulas.

Lemma 9.3 *Let φ, ψ be state formulas of CTL^* with $\llbracket\varphi\rrbracket = p \cdot \top$ and $\llbracket\psi\rrbracket = q \cdot \top$ for suitable tests p, q.*

1. $[\![\varphi \mathsf{U} \psi]\!] = (p \cdot \mathsf{n})^* \cdot q \cdot \top = ([\![\varphi]\!] \sqcap \mathsf{n})^* \cdot [\![\psi]\!]$.
2. $[\![\mathsf{G}\psi]\!]_i = (q \cdot \mathsf{n})^\omega$. *Hence we have the "shunting rule"* $(q \cdot \mathsf{n})^\omega = \neg_i (\mathsf{n}^* \cdot \neg q \cdot \mathsf{N})$.

Proof.

1. Using Theorem 5.6, (7) and Lm. 3.5.7 we calculate

$$[\![\varphi \mathsf{U} \psi]\!] = \mu y \,.\, q \cdot \top + (p \cdot \top \sqcap \mathsf{n} \cdot y) = \mu y \,.\, q \cdot \top + p \cdot \mathsf{n} \cdot y,$$

and the claim follows by Def. 3.1.4.

2. First we note that $[\![\varphi]\!]_i = p \cdot \mathsf{N}$ and $[\![\psi]\!]_i = q \cdot \mathsf{N}$ by Th. 9.1.2.
By Th. 7.6.5 and (7) $[\![\mathsf{G}\psi]\!]_i = \nu f^\circ_{\mathsf{N},[\![\neg\psi]\!]_i}$ where $f^\circ_{\mathsf{N},[\![\neg\psi]\!]_i}(y) =_{df} [\![\neg\psi]\!]_i \,\Box_i\, y$ for $y \in \mathsf{infel}(S)$. Since ψ is a state formula, f simplifies by Th. 9.1.2, Lm. 3.5.7 and Lm. 7.4.1 to

$$f(y) = [\![\psi]\!]_i \sqcap \mathsf{n} \cdot y = q \cdot \mathsf{N} \sqcap \mathsf{n} \cdot y = \mathsf{inf}\,(q \cdot \mathsf{n} \cdot y)\ .$$

To show the first claim we use ν-fusion (20) with $g = \mathsf{inf}$ and $h(y) = q \cdot \mathsf{n} \cdot y$. The function g is co-continuous by Lm. 7.4.3 and trivially satisfies $g(\top) = \mathsf{N} \geq \nu h$. Moreover, by the definitions of g, h, idempotence of inf, Lm. 7.2.2 and the definitions of f, g,

$$g(h(y)) = \mathsf{inf}\,(q \cdot \mathsf{n} \cdot y) = \mathsf{inf}\,(\mathsf{inf}\,(q \cdot \mathsf{n} \cdot y)) = \mathsf{inf}\,(q \cdot \mathsf{n} \cdot \mathsf{inf}\, y) = f(g(y))\ .$$

Hence, by ν-fusion (20) and the definitions of g and h,

$$[\![\mathsf{G}\psi]\!]_i = \nu f = g(\nu h) = \mathsf{inf}\,(q \cdot \mathsf{n})^\omega = (q \cdot \mathsf{n})^\omega\ ,$$

where the last step follows from Lm. 7.4.2 and n-generatedness, since

$$(q \cdot \mathsf{n})^\omega \leq \mathsf{n}^\omega = \mathsf{inf}\,\mathsf{n}^\omega \leq \mathsf{N}$$

by isotony and Lms. 8.3.3 and 7.4.1.
For the second claim we calculate, using the first claim, the definition of G, Th. 7.6.3, Th. 7.6.5, Th. 7.6.3 again, Lm. 7.2.2 with Def. 7.1, and Th. 9.1.2,

$$\begin{aligned}(q \cdot \mathsf{n})^\omega &= [\![\mathsf{G}\psi]\!]_i = [\![\neg\mathsf{F}\neg\psi]\!]_i = \neg_i\, [\![\mathsf{F}\neg\psi]\!]_i = \neg_i\, (\mathsf{n}^* \cdot [\![\neg\psi]\!]_i) \\ &= \neg_i\, (\mathsf{n}^* \cdot (\neg_i\, [\![\psi]\!]_i)) = \neg_i\, (\mathsf{n}^* \cdot (\neg_i\, (q \cdot \mathsf{N}))) = \neg_i\, (\mathsf{n}^* \cdot \neg q \cdot \mathsf{N})\ .\end{aligned}$$

□

Now we deal with EX.

Lemma 9.4 *For a state formula* φ *we have* $[\![\mathsf{EX}\varphi]\!] = [\![\mathsf{EXE}\varphi]\!]$ *and hence* $[\![\mathsf{EX}\varphi]\!]_i = [\![\mathsf{EXE}\varphi]\!]_i$.

Proof. By Def. 4.1, locality (Lm. 3.5.5), Lm. 3.5.4, neutrality of 1, locality again and Def. 4.1,

$$[\![\mathsf{EXE}\varphi]\!] = {}^\ulcorner(\mathsf{n} \cdot {}^\ulcorner[\![\varphi]\!] \cdot \top) \cdot \top = {}^\ulcorner(\mathsf{n} \cdot {}^\ulcorner[\![\varphi]\!]) \cdot \top = {}^\ulcorner(\mathsf{n} \cdot [\![\varphi]\!]) \cdot \top = [\![\mathsf{EX}\varphi]\!]\ .$$

□

We conclude this section by noting that in the infinitary semantics EX and AX are De Morgan duals.

Lemma 9.5 $[\![\mathsf{AX}\varphi]\!]_i = [\![\neg\mathsf{EX}\neg\varphi]\!]_i$.

Proof. By definition of A, Th. 7.6.3, Def. 7.5, Lemma 8.3.2 and Th. 7.6.4, Def. 7.5, and Th. 7.6.3, we obtain

$$\begin{aligned}[\![\mathsf{AX}\varphi]\!]_i &= [\![\neg\mathsf{E}\neg\mathsf{X}\varphi]\!]_i = \neg_i\,[\![\mathsf{E}\neg\mathsf{X}\varphi]\!]_i = \neg_i\,(\ulcorner[\![\mathsf{E}\neg\mathsf{X}\varphi]\!]_i \cdot \mathsf{N})\\ &= \neg_i\,(\ulcorner[\![\mathsf{EX}\neg\varphi]\!]_i \cdot \mathsf{N}) = \neg_i\,[\![\mathsf{EX}\neg\varphi]\!]_i = [\![\neg\mathsf{EX}\neg\varphi]\!]_i.\end{aligned}$$

□

From this and Lm. 9.4 we obtain the last result of this section.

Corollary 9.6 $[\![\mathsf{AX}\varphi]\!]_i = [\![\mathsf{AXA}\varphi]\!]_i$.

10 From CTL^* to CTL

For a number of applications the sublogic CTL of CTL^* suffices. We will see that it can be modelled in plain Kleene algebra. Syntactically, CTL consists of the CTL^* state formulas that use path formulas of the restricted form

$$\Pi \ ::= \ \mathsf{X}\,\Xi \mid \Xi\,\mathsf{U}\,\Xi \ . \tag{10}$$

From the previous section we already know that the semantics of every CTL formula is a test ideal t, from which, by Theorem 9.1.1, we can extract the corresponding test (or state set) as $\ulcorner t$. This is reflected by the simplified semantics $[\![\varphi]\!]_d =_{df} \ulcorner([\![\varphi]\!]_i)$ which enables us to calculate solely with tests.

Throughout this section we assume $\ulcorner\mathsf{N} = 1$, so that by locality (Lm. 3.5.5) $\ulcorner(a \cdot \mathsf{N}) = \ulcorner a$ for all a.

First we state another homomorphic property.

Lemma 10.1 *Over a complete Boolean semiring S the structure $(\mathsf{test}(S), \Box_d)$ with $p \Box_d q =_{df} |p \cdot \mathsf{n}\rangle q$ is an iteration algebra and $\ulcorner : \mathsf{rtest}(S) \to \mathsf{test}(S)$ is a homomorphism from $(\mathsf{rtest}(S), \Box_i)$ to $(\mathsf{test}(S), \Box_d)$. Moreover, $p \boxast_d q = |(p \cdot \mathsf{n})^*\rangle q$.*

Proof. By the remark following Def. 3.3 the set $\mathsf{test}(S)$ is downward closed and hence a complete lattice itself. Moreover, $\Box_d$ is isotone by isotony of $\cdot$ and diamond. By Lm. 3.5.1 $\ulcorner$ is continuous and strict. Finally, by definition of $\Box_i$ (Th. 7.6.1), Lm. 3.5.7, locality (Lm. 3.5.5) with the assumption $\ulcorner\mathsf{N} = 1$ and the definition of diamond,

$$\begin{aligned}\ulcorner((p \cdot \mathsf{N}) \Box_i (\mathsf{n} \cdot q \cdot \mathsf{N})) &= \ulcorner(p \cdot \mathsf{N} \sqcap \mathsf{n} \cdot q \cdot \mathsf{N}) = \ulcorner(p \cdot \mathsf{n} \cdot q \cdot \mathsf{N})\\ &= \ulcorner(p \cdot \mathsf{n} \cdot q) = |p \cdot \mathsf{n}\rangle q = p \Box_d q \ .\end{aligned} \tag{11}$$

Finally, by (7) $p \boxast_d q = \mu f_{p,q}$ where

$$f_{p,q}(x) = p \Box_d x + q = |p \cdot \mathsf{n}\rangle x + q \ ,$$

from which the claim follows by diamond star induction(Lm. 3.5.11). □

For the Boolean connectives we obtain by disjunctivity of domain and Lm. 3.5 together with Th. 7.6.3 and standard domain properties,

$$\llbracket \varphi \vee \psi \rrbracket_d = \llbracket \varphi \rrbracket_d + \llbracket \psi \rrbracket_d, \quad \llbracket \varphi \wedge \psi \rrbracket_d = \llbracket \varphi \rrbracket_d \cdot \llbracket \psi \rrbracket_d, \quad \llbracket \neg \varphi \rrbracket_d = \neg \llbracket \varphi \rrbracket_d. \tag{12}$$

Next, we state some laws for A.

Lemma 10.2 *For atomic proposition* $p \in \mathsf{test}(S)$*,*

$$\begin{aligned} \llbracket \mathsf{A}\bot \rrbracket_d &= 0, & \llbracket \mathsf{A}\top \rrbracket_d &= 1, \\ \llbracket \mathsf{A}(p \vee \varphi) \rrbracket_d &= p + \llbracket \mathsf{A}\varphi \rrbracket_d, & \llbracket \mathsf{A}(p \wedge \varphi) \rrbracket_d &= p \cdot \llbracket \mathsf{A}\varphi \rrbracket_d. \end{aligned}$$

Now we can calculate $\llbracket \_ \rrbracket_d$ for all CTL formulas by induction on their syntactic structure, cf. the grammar in (10).

Theorem 10.3

1. $\llbracket \bot \rrbracket_d = 0$.
2. $\llbracket p \rrbracket_d = p$.
3. $\llbracket \varphi \to \psi \rrbracket_d = \llbracket \varphi \rrbracket_d \to \llbracket \psi \rrbracket_d$.
4. $\llbracket \mathsf{EX}\varphi \rrbracket_d = |\mathsf{n}\rangle \llbracket \varphi \rrbracket_d$.
5. $\llbracket \mathsf{AX}\varphi \rrbracket_d = |\mathsf{n}] \llbracket \varphi \rrbracket_d = \llbracket \mathsf{AXA}\varphi \rrbracket_d$.
6. $\llbracket \mathsf{E}(\varphi \mathsf{U} \psi) \rrbracket_d = |(\llbracket \varphi \rrbracket_d \cdot \mathsf{n})^*\rangle \llbracket \psi \rrbracket_d$.
7. $\llbracket \mathsf{A}(\varphi \mathsf{U} \psi) \rrbracket_d = \neg \ulcorner \overline{(\mathsf{n}^* \cdot \llbracket \psi \rrbracket_d \cdot \mathsf{N})} \cdot |(\neg \llbracket \psi \rrbracket_d \cdot \mathsf{n})^*](\llbracket \varphi \rrbracket_d + \llbracket \psi \rrbracket_d)$.

Parts 4 and 5 mean that the existential and universal quantifiers of CTL are semantically reflected as the existential and universal modal operators diamond and box. Part 6 means that the starting states of the traces in $\llbracket \mathsf{E}(\varphi \mathsf{U} \psi) \rrbracket_d$ are precisely those from which after finitely many X steps through φ states a ψ state can be reached. Part 7 characterises $\llbracket \mathsf{A}(\varphi \mathsf{U} \psi) \rrbracket_d$ as the set of those states from which eventually a ψ state must be reached and for which iteration through non-ψ states must lead to a φ or a ψ state.

Proof. The proof is again by induction on the structure of the state formulas. The cases 1–3 of $\bot$, p and $\varphi \to \psi$ have already been covered in the proof of Theorem 9.1.

4. By the grammar (10), φ must be a state formula. Using Thm. 9.1.3, the definition of $\llbracket\ \rrbracket$, locality (Lm. 3.5.5 and the definition of $\llbracket\ \rrbracket$ again, we calculate $\llbracket \mathsf{EX}\varphi \rrbracket_d = \ulcorner \llbracket \mathsf{X}\varphi \rrbracket_i = \ulcorner(\mathsf{n} \cdot \llbracket \varphi \rrbracket_i) = \ulcorner(\mathsf{n} \cdot \ulcorner \llbracket \varphi \rrbracket_i) = |\mathsf{n}\rangle \llbracket \varphi \rrbracket_d$.
5. By the grammar (10), φ must be a state formula. By the definition of A, Thm. 7.6.4, Eq. (12), Part 4, Eq. (12), and the definition of box:

   $$\llbracket \mathsf{AX}\varphi \rrbracket_d = \llbracket \neg \mathsf{E} \neg \mathsf{X} \varphi \rrbracket_d = \llbracket \neg \mathsf{EX} \neg \varphi \rrbracket_d = \neg \llbracket \mathsf{EX} \neg \varphi \rrbracket_d = \neg |\mathsf{n}\rangle \llbracket \neg \varphi \rrbracket_d = \neg |\mathsf{n}\rangle \neg \llbracket \varphi \rrbracket_d = |\mathsf{n}] \llbracket \varphi \rrbracket_d\ .$$

   The second claimed equality holds, since $\llbracket \varphi \rrbracket_d = \llbracket \mathsf{A}\varphi \rrbracket_d$ follows from Thm. 9.1.4.
6. By the grammar (10), φ and ψ must be state formulas.
   Hence the claim is immediate from Lm. 10.1 and Lm. 5.4.

7. Again, by the grammar (10), φ and ψ must be state formulas.
We use that, by Cor. 4.2 and Lm. 3.5.4, $r = \neg\ulcorner\overline{u}$, where $u =_{df} [\![\varphi \mathsf{U} \psi]\!]_i$. Let, for abbreviation, $p \cdot \mathsf{N} =_{df} [\![\varphi]\!]_i$ and $q \cdot \mathsf{N} =_{df} [\![\psi]\!]_i$. Since $u = \mu f$ with $f(y) = q \cdot \mathsf{N} + p \cdot \mathsf{n} \cdot y$, we have by Lm. 13.4 that $\overline{u} = \nu f^\circ$ where f° is the De Morgan dual of f. We calculate the explicit form of f°. By the definitions, De Morgan, Lm. 3.5.8, Lm. 3.5.7 and De Morgan, Lm. 3.5.8 with Th. 7.6.4, Th. 7.6.2 and $y \in \mathsf{infel}(S)$, distributivity, and De Morgan:

$$\begin{aligned} f^\circ(y) &= \neg_i (q \cdot \mathsf{N} + p \cdot \mathsf{n} \cdot \neg_i y) = \neg_i (q \cdot \mathsf{N}) \sqcap \neg_i (p \cdot \mathsf{n} \cdot \neg_i y) = \neg q \cdot \mathsf{N} \sqcap \neg_i (p \cdot \mathsf{N} \sqcap \mathsf{n} \cdot \neg_i y) \\ &= \neg q \cdot (\neg_i (p \cdot \mathsf{N}) + \neg_i (\mathsf{n} \cdot \neg_i y)) = \neg q \cdot (\neg p \cdot \mathsf{N} + \neg_i \neg_i (\mathsf{n} \cdot y)) = \neg q \cdot (\neg p \cdot \mathsf{N} + \mathsf{n} \cdot y) \\ &= \neg q \cdot \neg p \cdot \mathsf{N} + \neg q \cdot \mathsf{n} \cdot y = \neg(p+q) \cdot \mathsf{N} + \neg q \cdot \mathsf{n} \cdot y . \end{aligned}$$

By the above, Def. 3.1.4, distributivity and De Morgan, Lm. 9.3.2 and a domain property, and Theorem 9.1.4 with the definition of box:

$$\begin{aligned} r &= \neg\ulcorner(\nu f^\circ) = \neg\ulcorner((\neg q \cdot \mathsf{n})^\omega + (\neg q \cdot \mathsf{n})^* \cdot \neg(p+q) \cdot \mathsf{N}) \\ &= \neg\ulcorner((\neg q \cdot \mathsf{n})^\omega) \cdot \neg\ulcorner((\neg q \cdot \mathsf{n})^* \cdot \neg(p+q) \cdot \mathsf{N}) = \\ \neg\ulcorner(\overline{\mathsf{n}^* \cdot q \cdot \mathsf{N}}) &\cdot \neg\ulcorner((\neg q \cdot \mathsf{n})^* \cdot \neg(p+q)) = \neg\ulcorner(\overline{\mathsf{n}^* \cdot q \cdot \mathsf{N}}) \cdot |(\neg q \cdot \mathsf{n})^*](p+q) . \end{aligned}$$

□

Corollary 10.4

$$\begin{aligned} [\![\mathsf{EF}\psi]\!]_d &= |\mathsf{n}^*\rangle [\![\psi]\!]_d , & [\![\mathsf{EG}\psi]\!]_d &= \ulcorner([\![\psi]\!]_d \cdot \mathsf{n})^\omega , \\ [\![\mathsf{AG}\psi]\!]_d &= |\mathsf{n}^*] [\![\psi]\!]_d , & [\![\mathsf{AF}\psi]\!]_d &= \neg\ulcorner(\neg[\![\psi]\!]_d \cdot \mathsf{n})^\omega = \neg\ulcorner\overline{\mathsf{n}^* \cdot [\![\psi]\!]_d \cdot \top} . \end{aligned}$$

Hence we can simplify the last property of Th. 10.3 to

$$[\![\mathsf{A}(\varphi \mathsf{U} \psi)]\!]_d = [\![\mathsf{AF}\psi]\!]_d \cdot |(\neg[\![\psi]\!]_d \cdot \mathsf{n})^*]([\![\varphi]\!]_d + [\![\psi]\!]_d) .$$

Proof. Immediate from Th. 10.3 and the definitions of F and G. □

Together with Th. 10.3 this shows that the sublogic CTL needs fewer algebraic concepts than full CTL^*: general joins and complementation (and therefore also general meet) are not needed. For the CTL semantics a modal left omega algebra [15] is sufficient. Further details, in particular the usual least-fixed-point characterisation of $[\![\mathsf{A}(\varphi \mathsf{U} \psi)]\!]_d$, can be found in [18].

11 From CTL^* to LTL

The logic LTL is the fragment of CTL^* in which only A may occur, once and outermost only, as path quantifier. More precisely, LTL has no state formulas apart from those of the form $\mathsf{A}\varphi$ and the path formulas are given by

$$\Pi ::= \Phi \mid \bot \mid \Pi \to \Pi \mid \mathsf{X}\,\Pi \mid \Pi \,\mathsf{U}\, \Pi .$$

Over an n-generated semiring, the LTL semantics is embedded into the CTL^* one by assigning to $\varphi \in \Pi$ the semantic value $[\![\mathsf{A}\varphi]\!]_i$.

The reason for this is the following. An arbitrary CTL^* formula φ may be called *valid* if its semantics is the set of all paths, abstractly, if $[\![\varphi]\!]_i = \mathsf{N}$. This is related to the A quantifier:

Lemma 11.1 $[\![\varphi]\!]_i = \mathsf{N} \Leftrightarrow [\![\mathsf{A}\varphi]\!]_i = \mathsf{N}$.

Proof. By Cor. 4.2 and neutrality of 1, Lm. 3.5.6, Boolean algebra, full strictness of domain (Lm. 3.5.2) and Boolean algebra,

$$\begin{aligned} [\![\mathsf{A}\varphi]\!]_i = \mathsf{N} &\Leftrightarrow \neg\ulcorner\overline{[\![\varphi]\!]_i} \cdot \mathsf{N} = 1 \cdot \mathsf{N} \Leftrightarrow \neg\ulcorner\overline{[\![\varphi]\!]_i} = 1 \\ &\Leftrightarrow \ulcorner\overline{[\![\varphi]\!]_i} = 0 \Leftrightarrow \overline{[\![\varphi]\!]_i} = 0 \Leftrightarrow [\![\varphi]\!]_i = \mathsf{N} \ . \end{aligned}$$

□

Although the infinitary semantics adequately reflects the standard LTL semantics, we present another view of the concrete case $S = \mathsf{TRC}(\Sigma)$ for some set Σ of states (cf. Ex. 3.2). Since we want to set up a similar connection to modal operators as in the CTL case (Th. 10.3), we embed the carrier set $\mathcal{P}(\Sigma^\infty)$ of $\mathsf{TRC}(\Sigma)$ into the relational semiring $\mathsf{REL}(\Sigma^\infty)$ by encoding every subset $U \subseteq \Sigma^\infty$ as the relational test $h(U) =_{df} \{(\sigma, \sigma) \mid \sigma \in U\}$.

Based on this we define another semantic mapping $[\![\ ]\!]_\mathsf{L}$ as

$$[\![\varphi]\!]_\mathsf{L} =_{df} h([\![\varphi]\!]_i) \ . \tag{13}$$

Next, we mimic the semantic element n relationally. In $\mathsf{TRC}(\Sigma)$ we had $\mathsf{n} = \Sigma.\Sigma$, which was used to "glue" transitions to the front of traces. In $\mathsf{REL}(\Sigma^\infty)$ we replace this by the relation $N =_{df} \{(\sigma, \sigma^1) \mid a \in S\}$. Now for a subset $U \subseteq \Sigma^\infty$,

$$h(\mathsf{n} \bowtie U) = |N\rangle h(U) \ . \tag{14}$$

This allows the construction of yet another semantic homomorphism.

Lemma 11.2 *The structure* $(\mathsf{test}(\mathsf{REL}(\Sigma^\infty)), \Box_\mathsf{L})$ *with* $P \Box_\mathsf{L} Q =_{df} P \,;\, |\mathsf{N}\rangle Q$ *is an iteration algebra and* h *from* (13) *is a homomorphism from* $(\mathcal{P}(S^\omega), \Box_i)$ *to* $(\mathsf{test}(\mathsf{REL}(\Sigma^\infty)), \Box_\mathsf{L})$.

Proof. As detailed in the proof of Lm. 10.1, $\mathsf{test}(\mathsf{REL}(\Sigma^\infty))$ is a complete lattice. Moreover, $\Box_\mathsf{L}$ is isotone by isotony of $\cap$ and diamond. Further, since in $\mathsf{REL}(\Sigma^\infty)$ multiplication ; is completely disjunctive in ts right argument as well, $|N\rangle$ is additive, continuous and strict. Finally, the homomorphic property of h w.r.t. the $\Box$ operators is immediate from (14). □

From this, Th.7.6 and Lm. 5.4 we obtain, with $\cdot = \bowtie$ and $\mathsf{N} = S^\omega$,

$$\begin{aligned} [\![\bot]\!]_\mathsf{L} &= \emptyset \ , & [\![\mathsf{X}\varphi]\!]_\mathsf{L} &= |N\rangle [\![\varphi]\!]_\mathsf{L} \ , \\ [\![p]\!]_\mathsf{L} &= h(p \cdot \mathsf{N}) \ , & [\![\varphi \,\mathsf{U}\, \psi]\!]_\mathsf{L} &= \mu Y \,.\, [\![\psi]\!]_\mathsf{L} \boxplus_\mathsf{L} [\![\varphi]\!]_\mathsf{L} \ , \\ [\![\varphi \to \psi]\!]_\mathsf{L} &= [\![\varphi]\!]_\mathsf{L} \to [\![\psi]\!]_\mathsf{L} \ . \end{aligned}$$

From the third equation we obtain, since $P \to Q = \neg P + Q$,

$$\begin{aligned} [\![\neg\varphi]\!]_\mathsf{L} &= \neg[\![\varphi]\!]_\mathsf{L} \ , & [\![\top]\!]_\mathsf{L} &= h(\mathsf{N}) \ , \\ [\![\varphi \vee \psi]\!]_\mathsf{L} &= [\![\varphi]\!]_\mathsf{L} + [\![\psi]\!]_\mathsf{L} & [\![\varphi \wedge \psi]\!]_\mathsf{L} &= [\![\varphi]\!]_\mathsf{L} \,;\, [\![\psi]\!]_\mathsf{L} \ . \end{aligned}$$

Moreover, we can simplify the U operator. Let $P =_{df} [\![\varphi]\!]_{\mathsf{L}}$ and $Q =_{df} [\![\psi]\!]_{\mathsf{L}}$. By $P, Q \in \mathsf{test}(\mathsf{REL}(S))$, definition of diamond and the import/export law from Lm. 3.5.10, and Lm. 3.5.11,

$$\mu y \,.\, Q + P \,;\, |N\rangle y \;= \mu y \,.\, Q + |P \,;\, N\rangle y \;= |(P \,;\, N)^*\rangle Q \;.$$

From this we obtain

$$[\![\varphi \,\mathsf{U}\, \psi]\!]_{\mathsf{L}} = |([\![\varphi]\!]_{\mathsf{L}} \,;\, N)^*\rangle [\![\psi]\!]_{\mathsf{L}} \;, \quad [\![\mathsf{F}\psi]\!]_{\mathsf{L}} = |N^*\rangle [\![\psi]\!]_{\mathsf{L}} \;, \quad [\![\mathsf{G}\psi]\!]_{\mathsf{L}} = |N^*] [\![\psi]\!]_{\mathsf{L}} \;.$$

This shows that for LTL we can weaken the requirements on the underlying semantic algebra even further, viz. to that of a modal Kleene algebra.

Finally we briefly resume the discussion on axiom (1) in this interpretation.

$$[\![\mathsf{X}\neg\varphi]\!]_{\mathsf{L}} = \neg[\![\mathsf{X}\varphi]\!]_{\mathsf{L}} \;\Leftrightarrow\; |N\rangle\neg[\![\varphi]\!]_{\mathsf{L}} = \neg|N\rangle[\![\varphi]\!]_{\mathsf{L}} \;\Leftrightarrow\; |N][\![\varphi]\!]_{\mathsf{L}} = |N\rangle[\![\varphi]\!]_{\mathsf{L}}$$

for all φ. This means that N has to be a total and deterministic relation, which is the case if the function $\lambda x \,.\, \mathsf{n} \cdot x$ is surjective and injective, i.e., a bijection. These properties hold for the element $\Sigma.\Sigma$ that generates Σ^ω.

Note that the condition $|N] = |N\rangle$ does not propagate to $|N^*]$ and $|N^*\rangle$, since these correspond to iterated conjunction and disjunction, resp.

12 Conclusion

We have provided a compact algebraic semantics for full CTL^* in the framework of modal quantales and shown that for the two sublogics CTL and LTL the semantics can be mapped to closed expressions using modal operators as well as Kleene star and ω-iteration. Compared with representations of CTL^* in the modal μ-calculus (e.g. [9]) the compactness is achieved, since in quantales the modal operators are defined for ω-regular expressions (and even more generally), not only for atomic actions. Moreover, we have shown that for CTL and LTL the requirements on the semantic algebra can be relaxed to that of an omega or even just a Kleene algebra, resp.

As a non-trivial application, the article [17] shows that the algebraic semantics developed in this paper can be transferred to the setting of Concurrent Kleene Algebras and hence allow temporal reasoning about sequential subthreads there.

Future research will concern use of the algebraic semantics for concrete calculations in case studies as well the extension from the current propositional case to the first-order one; for this Tarskian frames as introduced in [14] seem promising candidates.

Acknowledgement We are grateful to Roland Glück for valuable comments.

References

1. R. C. Backhouse et al.: Fixed point calculus. Inform. Proc. Letters, 53:131–136 (1995)
2. J. Conway: Regular Algebra and Finite Machines. Chapman&Hall 1971
3. J. Desharnais, B. Möller: Characterizing determinacy in Kleene algebras. Information Sciences, 139, 253–273 (2001)
4. J. Desharnais, B. Möller: Non-Associative Kleene Algebra and Temporal Logics. `https://www.informatik.uni-augsburg.de/lehrstuehle/dbis/pmi/publications/all_pmi_tech-reports/tr-RAMiCS16`
5. J. Desharnais, B. Möller, G. Struth: Kleene algebra with domain. ACM Transactions on Computational Logic 7, 798–833 (2006)
6. R.M. Dijkstra: Computation calculus bridging a formalisation gap. Science of Computer Programming 37, 3–36 (2000)
7. E.A. Emerson: Temporal and modal logic. In J. van Leeuwen (ed.): Handbook of theoretical computer science. Vol. B: Formal models and semantics. Elsevier 1991, 995–1072
8. M. Ern, J. Koslowski, A. Melton, G. E. Strecker: A primer on Galois connections. In: Proc. 1991 Summer Conference on General Topology and Applications in Honor of Mary Ellen Rudin and Her Work. Annals of the New York Academy of Sciences 704, 103–125 (1993)
9. D. Harel, D. Kozen, J. Tiuryn: Dynamic Logic. MIT Press, 2000
10. S. Kleene: Introduction to metamathematics. Van Nostrand 1952
11. S. Kleene: Representation of events in nerve nets and finite automata. In C. Shannon, J. McCarthy (eds.): Automata Studies. Princeton University Press 1956, 3–41
12. D. Kozen: A completeness theorem for Kleene algebras and the algebra of regular events. Information and Computation 110, 366–390 (1994)
13. D. Kozen: Kleene algebras with tests. ACM Transactions on Programming Languages and Systems 19, 427–443 (1997)
14. D. Kozen: Some results in dynamic model theory. Science of Computer Programming 51, 3–22 (2004)
15. B. Möller: Lazy Kleene algebra. In D. Kozen (ed.): Mathematics of Program Construction. LNCS 3125. Springer 2004, 252–273. Revised version in [16]
16. B. Möller: Kleene getting lazy. Science of Computer Programming 65, 195–214 (2007)
17. B. Möller, C.A.R. Hoare: Exploring an interface model for CKA. In R. Hinze, J. Voigtländer (eds.): Mathematics of Program Construction. LNCS 9129. Springer 2015, 1–29
18. B. Möller, P. Höfner, and G. Struth: Quantales and temporal logics. In M. Johnson and V. Vene (eds.): Algebraic Methodology and Software Technology (AMAST 2006). LNCS 4019. Springer 2006, 263–277
19. K. Rosenthal: Quantales and their applications. Pitman Research Notes in Math. No. 234 Longman Scientific and Technical 1990
20. G. Schmidt and T. Ströhlein. *Relations and Graphs: Discrete Mathematics for Computer Scientists*. EATCS Monographs on Theoretical Computer Science. Springer, 1993.
21. A. Tarski: A lattice-theoretical fixpoint theorem and its applications. Pacific Journal of Mathematics, 5:285–309, 1955

13 Appendix: Elements of Fixed Point Theory

We recapitulate some basic facts fixed point theory.

Definition 13.1 Let f be an endofunction on a poset $(M, \leq)$.

1. An element $x \in M$ is a *pre-fixed point* of f if $f(x) \leq x$. The notion of *post-fixed point* is order-dual, and x is a *fixed point* of f if it is both a pre- and a post-fixed point. The set of all fixed points of f is denoted by $\mathsf{fix}\, f$.
2. An element is called the *least (pre-)fixed point* of f if it is the least element of the set of (pre-)fixed points of f. The notion of *greatest (post-)fixed point* is order-dual. Note that neither of these elements need exist.
3. The least and greatest fixed points of f are denoted by μf and νf, resp., when they exist. If $f(x) = E$, where E is an expression containing the variable x, we write $\mu x\,.\,E$ and $\nu x\,.\,E$ instead of μf and νf.

The following fundamental theorem, in particular Part 4, is due to Knaster and Tarski [21].

Theorem 13.2 (Knaster/Tarski) *Consider a partial order $(M, \leq)$ and an isotone endofunction $f : M \to M$.*

1. *If $u \in M$ is the least pre-fixed point of f then $u = \mu f$, i.e., u is also the least fixed point of f. Hence, if μf is known to exist we have the principle of* least fixed point induction*:*

$$f(x) \leq x \Rightarrow \mu f \leq x \ . \tag{15}$$

2. *Analogously, if the greatest post-fixed point of f exists then it is also the greatest fixed point νf of f. Hence if νf is known to exist we have the principle of* greatest fixed point co-induction*:*

$$x \leq f(x) \Rightarrow x \leq \nu f \ . \tag{16}$$

3. *Let also $g : M \to M$ be isotone and satisfy $f \leq g$, i.e., $\forall\, x : f(x) \leq g(x)$. If the set of pre-fixed points of f has a least element μf then $\mu f \leq u$ for every pre-fixed point u of g. In particular, if μg exists then $\mu f \leq \mu g$. Analogously, if g has a greatest post-fixed point νg, then also $u \leq \nu g$ for every post-fixed point u of f. In particular, if νf exists then $\nu f \leq \nu g$.*
4. *If $(M, \leq)$ is even a complete lattice then μf and νf exist and satisfy*

$$\begin{array}{lllll} \mu f & = & \bigsqcap \{x \,|\, f(x) = x\} & = & \bigsqcap \{x \,|\, f(x) \leq x\} \ , \\ \nu f & = & \bigsqcup \{x \,|\, f(x) = x\} & = & \bigsqcup \{x \,|\, x \leq f(x)\} \ . \end{array}$$

In the case of a Boolean lattice, least and greatest fixed points can be related via the dual functions.

Definition 13.3 Let $f : M \to N$ be a function between Boolean algebras M, N. The *dual function* of f, denoted f°, is defined by $f^\circ(x) =_{df} \overline{f(\overline{x})}$.

Lemma 13.4 *Let f be a function on a Boolean lattice. If μf exists then also νf° exists and $\nu f^\circ = \overline{\mu f}$. Likewise, if νf exists then also μf° exists and $\mu f^\circ = \overline{\nu f}$.*

We now mention two very useful groups of fixed point fusion laws (see e.g. [1] for further fixed point properties). They allow fusing the application of some function g with the recursion described by a function h, yielding a recursion described by a function f. Let $f, g, h : L \to L$ be isotone functions on a complete lattice $(L, \leq)$ with least element $\bot$ and greatest element $\top$. Then we have the *μ-super-fusion* law

$$g \circ h \geq f \circ g \;\Rightarrow\; g(\mu h) \geq \mu f \ . \tag{17}$$

If g is *continuous*, i.e., preserves suprema of non-empty chains, and satisfies $g(\bot) \leq \mu h$ then we have the *μ-sub-fusion and μ-fusion* laws

$$g \circ h \leq f \circ g \;\Rightarrow\; g(\mu h) \leq \mu f \ , \qquad g \circ h = f \circ g \;\Rightarrow\; g(\mu h) = \mu f \ . \tag{18}$$

Dually we have the *ν-sub-fusion* law

$$g \circ h \leq f \circ g \;\Rightarrow\; g(\nu h) \leq \nu f \ . \tag{19}$$

If g is *co-continuous*, i.e., preserves infima of non-empty chains, and satisfies $g(\top) \geq \nu h$ then we have the *ν-super-fusion and ν-fusion* laws

$$g \circ h \geq f \circ g \;\Rightarrow\; g(\nu h) \geq \nu f \ , \qquad g \circ h = f \circ g \;\Rightarrow\; g(\nu h) = \nu f \ . \tag{20}$$

The notion of (co-)continuity has another important application which is due to Kleene in [10].

Theorem 13.5 (Kleene) *Assume again a complete lattice L and an endofunction $f : L \to L$. For $x \in L$ set $f^0(x) =_{df} x$ and $f^{i+1}(x) =_{df} f(f^i(x))$. If f is continuous then*

$$\mu f \;=\; \bigsqcup \{f^i(\bot) \mid i \in \mathbb{N}\} \ ,$$

where $f^0(\bot) =_{df} \bot$ and $f^{i+1}(\bot) =_{df} f(f^i(\bot))$. Dually, if f is co-continuous then

$$\nu f \;=\; \bigsqcap \{f^i(\top) \mid i \in \mathbb{N}\}$$

This allows iterative computation of μf and νf.