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. We introduce new variants of Kleene star and omega iteration for the case where the iterated operator is neither associative nor has a neutral element. The associated *repetition algebras* are used to give closed semantic expressions for the *Until* and *While* operators of the temporal logic CTL^* and its sublogics CTL and LTL. Moreover, the relation between the semantics of these logics can be expressed by homomorphisms between repetition algebras, which is a more systematic and compact approach than the ones taken in earlier papers.

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

1 Introduction

The temporal logic CTL^* and its sublogics CTL and LTL (see [7] for an excellent survey) are prominent tools in the analysis of concurrent and reactive systems. Although they are well understood, one still rarely finds algebraic treatments of their semantics which provide a better understanding and yield simpler (and, at the same time, completely formal) proofs of the semantic properties.

In the present paper we take up the approach of [15] 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 repetition algebras. The relation between various semantics for CTL* and CTL can then be expressed by homomorphisms between repetition algebras; in particular, several tedious ad-hoc applications of the principle of least/greatest fixed point fusion that occurred in [15] are now replaced by a single proof for general repetition 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 trace quantifier A and the globality operator G arise. For lack of space we omit all proofs; they are found in the report [4].

2 Modelling CTL^*

To make the paper self-contained we recall some basic facts about CTL^*; in this we largely follow [7]. 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* 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 traces, and X and U are the next-time and until operators.

We briefly recall the informal semantics. A trace is said to satisfy an atomic formula iff its first state does. A trace σ satisfies $\mathsf{E}\varphi$ iff there is some trace τ that satisfies φ and has the same first state as σ. The formula $\mathsf{X}\varphi$ holds for a trace σ if φ holds 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 *trace formulas*[4] 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 words over some set Σ of states. 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 holds. The relation $\sigma \models \varphi$ of *satisfaction* of a formula φ by a trace σ is defined inductively (see e.g. [7]) by

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

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

---

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

[4] In the literature these are mostly called *path formulas*.

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 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* [12] 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 [12].
5. The IL-semiring/left quantale is *Boolean* if $(A, \leq)$ induces a Boolean algebra.

Quantales (or *standard Kleene algebras* [2]) have been used in many contexts other than that of program semantics (cf. the general reference [16]). 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 [9] only special cases of it, like the induction and co-induction 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 V of traces are $\mathsf{inf}\, V =_{df} V \cap \Sigma^\omega$ and $\mathsf{fin}\, V =_{df} V - \mathsf{inf}\, V$. With this we extend $\bowtie$ to trace sets V, W as

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

This operation has the set Σ, viewed as a set of one-element traces, as its neutral element. Moreover, $V \bowtie \emptyset = \mathsf{inf}\, V$ and hence $V \bowtie \emptyset = \emptyset$ iff $\mathsf{inf}\, V = \emptyset$. 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 has the greatest element $\top = \Sigma^\infty$ and is even left-distributive. A transition relation over a state set Σ can be modelled in $\mathsf{TRC}(\Sigma)$ as a set R of words 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 $\Sigma^2 =_{df} \Sigma.\Sigma$, the set of all two-letter words and hence the most general next-step transition relation. Then $\mathsf{TRC}(\Sigma)$ is generated by Σ^2 as $\mathsf{TRC}(\Sigma) = (\Sigma^2)^* \cup (\Sigma^2)^\omega$. This is generalised in Sect. 8. $\square$

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 [10].

Definition 3.3 A *test* in an IL-semiring is an element p that has a complement $\neg p$ relative to 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 $\neg p = \overline{p} \sqcap 1$, where $^{-}$ is the general complement operator (that need not exist in non-Boolean IL-semirings). 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.

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

Using tests we can also define a domain operator and the modal operators diamond and box (cf. [5]). Due to the existence of $\top$ we can use a slightly different but equivalent axiomatisation than given there; the equivalence is established by Lemma 9.1 of that paper.

Definition 3.4 A bounded IL-semiring A is called a *domain IL-semiring* if it has a *domain operator* $\ulcorner : A \to \mathsf{test}(A)$ axiomatised, for $a, b \in A, q \in \mathsf{test}(A)$, by the Galois connection $\ulcorner a \leq q \Leftrightarrow a \leq q \cdot \top$ together with the axiom of *locality*

$$\ulcorner(a \cdot b) = \ulcorner(a \cdot \ulcorner b)\ . \tag{2}$$

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

The locality property means that the domain of a composition does not depend on the inner structure of the second operand, but only on its starting states.

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

We recall a few basic properties; see [5] for more details).

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

1. $a = \ulcorner a \cdot a$ *and* $\ulcorner(p \cdot a) \leq p$.
2. $\ulcorner(p \cdot \top) = p$.
3. $p \leq q \Leftrightarrow p \cdot \top \leq q \cdot \top$.
4. *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,* $p \cdot \top \sqcap b = p \cdot b$.
5. *If A is Boolean then* $\neg p \cdot \top = \overline{p \cdot \top}$.
6. $|a \cdot b\rangle q = |a\rangle(|b\rangle q)$ *and* $|a \cdot b]q = |a](|b]q)$.
7. $p \cdot |b\rangle q = |p \cdot b\rangle q$ *(import/export).*
8. $p \leq q \cdot |a]p \Rightarrow p \leq |a^*]q$ *(box induction).*

By these properties we can represent the set of all possible traces that start with some state in set p by the *test ideal* $p \cdot \top$. By Part 3 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 domain quantale A. 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 traces that satisfy it.

$$
\begin{aligned}
[\![\bot]\!] &= \emptyset\ , & [\![\mathsf{E}\varphi]\!] &= \ulcorner[\![\varphi]\!] \bowtie \Sigma^\omega\ ,\\
[\![\pi]\!] &= \Sigma_\pi \bowtie \Sigma^\omega\ , & [\![\mathsf{X}\,\varphi]\!] &= \Sigma^2 \bowtie [\![\varphi]\!]\ ,\\
[\![\varphi \to \psi]\!] &= \overline{[\![\varphi]\!]} \cup [\![\psi]\!]\ , & [\![\varphi\,\mathsf{U}\,\psi]\!] &= \bigcup_{j \geq 0} ((\Sigma^2)^j \bowtie [\![\psi]\!] \cap \bigcap_{k<j} (\Sigma^2)^k \bowtie [\![\varphi]\!])\ .
\end{aligned}
$$

Note that in Σ^2 the power is taken w.r.t. the concatenation operator . whereas j and k denote powers w.r.t. $\bowtie$.

As 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 $\Phi = \mathsf{test}(A)$. Moreover, we fix an element x (where x stands for "next" and corresponds to Σ^2) that represents the transition system underlying the logic. The precise requirements for x will be discussed in Sect. 6. Then the concrete semantics above generalises to a function $[\![\_]\!] : \Psi \to A$, where $[\![\varphi]\!]$ abstractly represents the set of traces 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:

$$\begin{array}{rlrl} [\![\bot]\!] &= 0\ , & [\![\mathsf{E}\varphi]\!] &= \ulcorner[\![\varphi]\!]\cdot\top\ , \\ [\![p]\!] &= p\cdot\top\ , & [\![\mathsf{X}\,\varphi]\!] &= \mathsf{x}\cdot[\![\varphi]\!]\ , \\ [\![\varphi\rightarrow\psi]\!] &= \overline{[\![\varphi]\!]}+[\![\psi]\!]\ , & [\![\varphi\,\mathsf{U}\,\psi]\!] &= \bigsqcup\limits_{j\geq 0}(\mathsf{x}^j\cdot[\![\psi]\!]\sqcap\bigsqcap\limits_{k<j}\mathsf{x}^k\cdot[\![\varphi]\!])\ . \end{array}$$

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 state a number of properties of the trace 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* $[\![\mathsf{A}\psi]\!]=\neg\ulcorner\overline{[\![\psi]\!]}\cdot\top$.

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

Lemma 4.3 $[\![\mathsf{EX}\top]\!]=\top\Leftrightarrow\ulcorner\mathsf{x}=1$.

In a relational setting the property $\ulcorner\mathsf{x}=1$ means that x is a left-total transition relation.

5 Modified Iteration and the Semantics of Until

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

$$a\,\boxed{j}\,b =_{df} \mathsf{x}^j\cdot b\sqcap\bigsqcap_{k<j}\mathsf{x}^k\cdot a\ , \qquad (4)$$

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, $a\,\boxed{0}\,b=\mathsf{x}^0\cdot b\sqcap\bigsqcap_{k<0}\mathsf{x}^k\cdot a=b\sqcap\top=b$. To proceed with the induction step we need an assumption about x that is closely related to (1), as is discussed in detail in Sect. 6. This condition reads

$$\forall\,a,b\in A:\mathsf{x}\cdot(a\sqcap b)=\mathsf{x}\cdot a\sqcap\mathsf{x}\cdot b\ . \qquad \text{(LDM)}$$

It means that left multiplication by x 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,

$$\begin{array}{rcl} a \boxed{j+1} b & = & \mathsf{x}^{j+1} \cdot b \sqcap \bigsqcap_{k<j+1} \mathsf{x}^k \cdot a \;=\; \mathsf{x}^{j+1} \cdot b \;\sqcap \mathsf{x}^0 \cdot a \sqcap \bigsqcap_{k=1}^{j} \mathsf{x}^k \cdot a \\ & = & a \sqcap \mathsf{x} \cdot \mathsf{x}^j \cdot b \sqcap \bigsqcap_{k=1}^{j} \mathsf{x} \cdot \mathsf{x}^{k-1} \cdot a \;=\; a \sqcap \mathsf{x} \cdot \mathsf{x}^j \cdot b \sqcap \bigsqcap_{l<j} \mathsf{x} \cdot \mathsf{x}^l \cdot a \\ & = & a \sqcap \mathsf{x} \cdot (\mathsf{x}^j \cdot b \sqcap \bigsqcap_{l<j} \mathsf{x}^l \cdot a) \;=\; a \sqcap \mathsf{x} \cdot (a \boxed{j} b) \;=\; a \mathbin{\Box} (a \boxed{j} b) \;, \end{array}$$

where

$$c \mathbin{\Box} d =_{df} c \boxed{1} d = c \sqcap \mathsf{x} \cdot d \; . \tag{5}$$

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

We can now formulate the semantics of until more compactly as

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

Below we will relate this to a fixed point equation for U.

The operator $\Box$ 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 $\Box : S \times S \to S$.

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

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

2. The structure $(S, \Box)$ is called a *repetition algebra*[5] if S is a complete lattice with order $\leq$, least element 0 and binary supremum operator $+$, and $\Box$ is isotone in both arguments.
3. In a repetition algebra we define variants of the star and omega operators:

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

In fact, $\boxed{*}$ corresponds to Kleene's original definition of $*$ as an infix operator in [8]. Not surprisingly, $\boxed{*}$ and $^{\boxed{\omega}}$ enjoy properties analogous to those of * and $^\omega$. We recall that an endofunction on a complete lattice is *(co-)continuous* if it preserves all joins (meets) of non-empty chains.

[5] We would have preferred the term *iteration algebra* which, however, is already used in [1] and follow-up papers with a different meaning.

Lemma 5.2 *Consider a repetition algebra* $(S, \Box)$.

1. *The operators* $\boxast$ *and* $^{\boxed{\omega}}$ *are isotone.*
2. $a \boxed{i+j} a = a \boxed{i} (a \boxed{j} b)$.
3. *If* $\Box$ *is right-strict, i.e., if* $a \Box 0 = 0$ *for all* a*, and distributes through arbitrary joins and binary meets in its right argument then* $f_{a,b}$ *from* (7) *is continuous and* $a \boxast b = \bigsqcup_{j \geq 0} a \boxed{j} b$.
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* $\nu f_{a,b} = \mu f_{a,b} + a^{\boxed{\omega}} = a \boxast b + a^{\boxed{\omega}}$.

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

Definition 5.3 Let $(S_i, \Box_i)_{i=1,2}$ be repetition 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 $h(a +_1 b) = h(a) +_2 h(b)$ 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 repetition algebras with a* homomorphism $h : S_1 \to S_2$. *Then* h *preserves* $\boxast$ *as well, i.e.,* $h(a \boxast_1 b) = h(a) \boxast_2 h(b)$ *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* $a \in S_1$.

We now return to the concrete instance of $\Box$ defined in (5). To make use of Lemma 5.2 we need to ensure that $\Box$ has the necessary properties. Fortunately, this is achieved by stipulating besides (LDM) a second requirement on the semantic element x, motivated by the semantics of X as follows. In $\mathsf{TRC}(\Sigma)$, for arbitrary formula φ and its semantics $V = [\![\varphi]\!]$ we want

$$[\![\mathsf{X}\varphi]\!] = \mathsf{x} \bowtie V = \mathsf{x} \bowtie \bigcup_{v \in V} \{v\} = \bigcup_{v \in V} \mathsf{x} \bowtie \{v\} \ .$$

Therefore, we require that in the abstract quantale semantics left multiplication by x distributes through arbitrary joins.

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

Now Lemma 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 domain quantale with a step* x. *Then*

$$[\![\varphi \,\mathsf{U}\, \psi]\!] = [\![\varphi]\!] \boxast [\![\psi]\!] \ .$$

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

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

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 $\overline{\mathsf{x} \cdot a} = [\![\neg \mathsf{X}\varphi]\!] = [\![\mathsf{X}\neg\varphi]\!] = \mathsf{x} \cdot \overline{a}$. 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* A *and* $\mathsf{x} \in A$.

1. *If* x *is left-distributive, i.e.,* $\mathsf{x} \cdot (a + b) = \mathsf{x} \cdot a + \mathsf{x} \cdot b$ *for all* a, b, *and satisfies* $\forall\, a \in A : \mathsf{x} \cdot \overline{a} \le \overline{\mathsf{x} \cdot a}$ *then* (LDM) *and* $\mathsf{x} \cdot 0 = 0$ *hold.*
2. *If* (LDM) *and* $\mathsf{x} \cdot 0 = 0$ *hold then so does* $\forall\, a \in A : \mathsf{x} \cdot \overline{a} \le \overline{\mathsf{x} \cdot a}$.
3. *If* x *is left-distributive then* $\forall\, a \in A : \overline{\mathsf{x} \cdot a} \le \mathsf{x} \cdot \overline{a} \Leftrightarrow \mathsf{x} \cdot \top = \top \Leftrightarrow \mathsf{x}^\omega = \top$.
4. *If* x *satisfies* (LDM) *and* $\forall\, a : \mathsf{x} \cdot \overline{a} = \overline{\mathsf{x} \cdot a}$ *then* x *is left-distributive.*

In relation algebra, the special case $\mathsf{x} \cdot \overline{1} \le \overline{\mathsf{x}}$ of the property in Part 1 characterises x as a partial function and is equivalent to the full property $\forall\, a : \mathsf{x} \cdot \overline{a} \le \overline{\mathsf{x} \cdot a}$ [17]. 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 TRC left multiplication by an element x distributes over meet iff x is prefix-free, i.e., if no member of x is a prefix of another member. This holds in particular if all words in x have equal length, which is the case if x models a transition relation and hence consists only of words of length 2. The equivalent condition $\forall\, a : \mathsf{x} \cdot a \sqcap \mathsf{x} \cdot \overline{a} = 0$ was used in the computation calculus of R.M. Dijkstra [6].

But what about Lemma 6.1.3? Only rarely will a quantale be "generated" by x in the sense that $\mathsf{x}^\omega = \top$. We deal with this problem in Sections 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 $A = \mathsf{TRC}(\Sigma)$. There we definitely do *not* have $\mathsf{x}^\omega = \top$ for $\mathsf{x} = \Sigma^2$, since $\mathsf{x}^\omega = \Sigma^\omega = \mathsf{inf}\, A$, where the inf operator was introduced in Ex. 3.2.

We will show that restricting the semantics given in Sect. 4 to infinite words remedies this 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 $V \bowtie \emptyset = \mathsf{inf}\, V$ and hence $V \bowtie \emptyset = \emptyset$ iff $\mathsf{inf}\, V = \emptyset$.

This motivates the following definition.

Definition 7.1 Assume a bounded IL-semiring A.

1. The *purely infinite part* of $a \in A$ is $\mathsf{inf}\, a =_{df} a \cdot 0$. We call *a purely infinite* or *non-terminating* if $a = \mathsf{inf}\, a$. We set $\mathsf{N} =_{df} \mathsf{inf}\, \top$; hence N is the greatest *n*onterminating element. The set of all purely infinite elements is denoted by $\mathsf{infel}(A)$.
2. Dually, we call *a purely finite* if $\mathsf{inf}\, a = a \cdot 0 \leq 0$, i.e., if its purely infinite part is trivial. The right hand side is equivalent to $a \cdot 0 = 0$.
3. If A is Boolean we can define the *purely finite part* of $a \in A$ 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 [12].

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

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* $p \in \mathsf{test}(A)$, $\mathsf{inf}\,(p \cdot b) = p \cdot \mathsf{inf}\, b$.
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* $\mathsf{inf} : A \to \mathsf{infel}(A)$.

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

Definition 7.3 The *infinitary semantics* $[\![\varphi]\!]_i$ of a CTL^* formula φ over a Boolean left domain 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 $\neg_i\, a =_{df} \mathsf{N} - a$. This satisfies the following properties.

Theorem 7.4 *Assume a Boolean left quantale* A *with a step* x.

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

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

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

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 7.5 *Assume again* $\mathsf{N} \leq \mathsf{x} \cdot \mathsf{N}$ *and define, for formulas* φ *and* ψ *the abbreviation* $\varphi\mathsf{W}\psi \Leftrightarrow_{df} \mathsf{G}\varphi \vee (\varphi\mathsf{U}\psi)$. *Then* $\llbracket \varphi\mathsf{W}\psi \rrbracket_i = \nu y\,.\,\llbracket\psi\rrbracket_i + (\llbracket\varphi\rrbracket_i \,\Box_i\, y)$.

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 with φ holding all the time before that.

8 Generated Quantales

In view of Theorem 7.4.4 we introduce a new notion.

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

The definition means that all elements of A can be obtained by finite or infinite iteration of x. The constraint $\mathsf{x}^\omega \leq \mathsf{N}$ serves to exclude "pseudo-infinite" iterations of x. 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 Σ^2-generated, while its reduct to finite traces is not. ☐

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

$$\mathsf{rtest}(A) \;=_{df}\; \{p \cdot \mathsf{N} \mid p \in \mathsf{test}(A)\} \tag{8}$$

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

Lemma 8.3 *Consider an* x-*generated quantale* A.

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

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

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

Assume now that A *is strongly* x*-generated.*

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

We can extend Lemma 8.3.5 a bit further. Together with Lemma 8.3.6 we obtain $[\![\mathsf{G}\psi]\!]_i = \bigsqcap_{i \in \mathbb{N}} \mathsf{x}^i \cdot [\![\psi]\!]_i$. Hence, in a $*$-continuous quantale [9], 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 $[\![\mathsf{F}\psi]\!]_i = \bigsqcup_{i \in \mathbb{N}} \mathsf{x}^i \cdot [\![\psi]\!]_i$ and $[\![\mathsf{G}\psi]\!]_i = \bigsqcap_{i \in \mathbb{N}} \mathsf{x}^i \cdot [\![\psi]\!]_i$.

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 x-generated quantale.

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

1. $[\![\varphi]\!]$ *is a test ideal, and hence, by Lemma 3.5.2,* $[\![\varphi]\!] = \ulcorner [\![\varphi]\!] \cdot \top$.
2. $[\![\varphi]\!]_i$ *is a relative test ideal, i.e,* $[\![\varphi]\!]_i = \ulcorner [\![\varphi]\!] \cdot \mathsf{N}$.
3. $[\![\mathsf{E}\varphi]\!] = [\![\varphi]\!]$.
4. $[\![\mathsf{A}\varphi]\!] = [\![\varphi]\!]$.

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* $\vee$.

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* $[\![\varphi]\!] = p \cdot \top$ *and* $[\![\psi]\!] = q \cdot \top$ *for suitable tests* p, q.

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

Now we deal with EX.

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

We conclude this section by noting that in the infinitary semantics EX and AX are De Morgan duals; again the proof is a straightforward calculation.

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

From this and Lemma 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 trace formulas of the restricted form

$$\Pi \ ::= \ \mathsf{X}\,\Xi \mid \Xi\,\mathsf{U}\,\Xi \ . \tag{9}$$

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[6] $[\![\varphi]\!]_d =_{df} \ulcorner([\![\varphi]\!]_i)$ which enables us to calculate solely with tests. Throughout this section we assume $\ulcorner\mathsf{N} = 1$, so that by locality (2) $\ulcorner(a \cdot \mathsf{N}) = \ulcorner a$ for all a.

First we state another homomorphic property.

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

For the Boolean connectives we obtain by disjunctivity of domain and Lemma 3.5 together with Theorem 7.4.3 and standard domain properties,

$$[\![\varphi \vee \psi]\!]_d = [\![\varphi]\!]_d + [\![\psi]\!]_d, \quad [\![\varphi \wedge \psi]\!]_d = [\![\varphi]\!]_d \cdot [\![\psi]\!]_d, \quad [\![\neg\varphi]\!]_d = \neg[\![\varphi]\!]_d. \tag{10}$$

Next, we state some laws for A.

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

$$[\![\mathsf{A}\bot]\!]_d = 0, \qquad [\![\mathsf{A}\top]\!]_d = 1,$$
$$[\![\mathsf{A}(p \vee \varphi)]\!]_d = p + [\![\mathsf{A}\varphi]\!]_d, \qquad [\![\mathsf{A}(p \wedge \varphi)]\!]_d = p \cdot [\![\mathsf{A}\varphi]\!]_d.$$

Now we can calculate $[\![\_]\!]_d$ for all CTL formulas by induction on their syntactic structure, cf. the grammar in (9). We use implication $\to$ between tests, defined as $p \to q =_{df} \neg p + q$.

Theorem 10.3

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

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 $[\![\mathsf{E}(\varphi\mathsf{U}\psi)]\!]_d$ are precisely those from which after finitely many X steps through φ states a ψ state can be reached. Part (7) characterises $[\![\mathsf{A}(\varphi\mathsf{U}\psi)]\!]_d$ 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.

[6] The subscript $_d$ stands for "domain".

11 From CTL^* to LTL

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

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

Over an x-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 traces, abstractly, if $[\![\varphi]\!]_i = \mathsf{N}$. This is related to the A quantifier:

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

Although the infinitary semantics adequately reflects the standard LTL semantics, we present another view of the concrete case $A = \mathsf{TRC}(\Sigma)$ 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 (Theorem 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 $V \subseteq \Sigma^\infty$ as the relational test $h(V) =_{df} \{(\sigma,\sigma) \mid \sigma \in V\}$.

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

$$[\![\varphi]\!]_{\mathsf{L}} =_{df} h([\![\varphi]\!]_i) \ . \tag{11}$$

Next, we mimic the semantic element x relationally. In $\mathsf{TRC}(\Sigma)$ we had $\mathsf{x} = \Sigma^2$, which was used to "glue" transitions to the front of traces. In $\mathsf{REL}(\Sigma^\infty)$ we replace this by the relation $N =_{df} \{(\sigma,\sigma^1) \mid \sigma \in \Sigma^\omega\}$, where, as in Section 2, σ^1 is σ with its first state removed. Now for a subset $V \subseteq \Sigma^\infty$,

$$h(\mathsf{x} \bowtie V) = |N\rangle h(V) \ . \tag{12}$$

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 a repetition algebra and* h *from* (11) *is a homomorphism from* $(\mathcal{P}(A^\omega), \Box_i)$ *to* $(\mathsf{test}(\mathsf{REL}(\Sigma^\infty)), \Box_{\mathsf{L}})$.

From this, Theorem7.4 and Lemma 5.4 we obtain, with $\cdot = \bowtie$, $\mathsf{N} = A^\omega$ and $P \to Q = \neg P + Q$ (P, Q relational tests),

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

From the last equation we obtain

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

Moreover, we can simplify the U operator. Let $P =_{df} [\![\varphi]\!]_{\mathsf{L}}$ and $Q =_{df} [\![\psi]\!]_{\mathsf{L}}$. By Lemma 11.2 with Lemma 5.4, definition of diamond with the import/export law from Lemma 3.5.7 and Lemma 3.5.8,

$$P \boxast_{\mathsf{L}} Q = \mu Y \,.\, Q + P \,;\, |N\rangle Y \ = \mu Y \,.\, Q + |P \,;\, N\rangle Y \ = |(P \,;\, N)^*\rangle Q \ .$$

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 $\lambda x \,.\, \mathsf{x} \cdot x$ is surjective and injective, i.e., a bijection. These properties hold for the element Σ^2 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 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 (Sections 9 and 10) or even just a Kleene algebra (Section 11).

As a non-trivial application, the article [14] 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 [11] seem promising candidates.

Acknowledgement We are grateful to Roland Glück and to the anonymous referees for valuable comments.

References

1. S. Bloom, Z. Ésik: Iteration algebras. Int. J. Found. Comput. Sci. 3:3, 245–302 (1992)
2. J. Conway: Regular Algebra and Finite Machines. Chapman&Hall 1971
3. J. Desharnais, B. Möller: Characterizing determinacy in Kleene algebras. Inf. Sci., 139, 253–273 (2001)
4. J. Desharnais, B. Möller: Non-associative Kleene algebra and temporal logics. `https://www.informatik.uni-augsburg.de/de/lehrstuehle/dbis/pmi/publications/all_pmi_tech-reports/tr-RAMICS16/`
5. J. Desharnais, B. Möller, G. Struth: Kleene algebra with domain. ACM Trans. on Comp. Logic 7, 798–833 (2006)
6. R.M. Dijkstra: Computation calculus bridging a formalisation gap. Sci. Comp. Prog. 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. 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
9. D. Kozen: A completeness theorem for Kleene algebras and the algebra of regular events. Inf. Comp. 110, 366–390 (1994)
10. D. Kozen: Kleene algebras with tests. ACM Trans. Prog. Lang. Systems 19, 427–443 (1997)
11. D. Kozen: Some results in dynamic model theory. Sci. Comp. Prog. 51, 3–22 (2004)
12. B. Möller: Lazy Kleene algebra. In D. Kozen (ed.): Mathematics of Program Construction. LNCS 3125. Springer 2004, 252–273. Revised version in [13]
13. B. Möller: Kleene getting lazy. Sci. Comp. Prog. 65, 195–214 (2007)
14. 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
15. 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
16. K. Rosenthal: Quantales and their applications. Pitman Research Notes in Math. No. 234 Longman Scientific and Technical 1990
17. G. Schmidt and T. Ströhlein. *Relations and Graphs: Discrete Mathematics for Computer Scientists*. EATCS Monographs on Theoretical Computer Science. Springer, 1993.