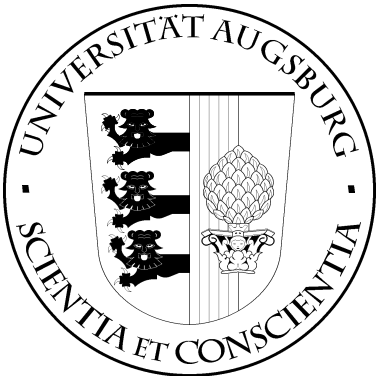
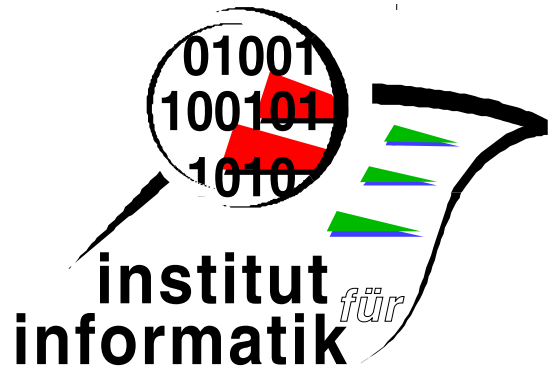
Universität Augsburg



Quantales and Temporal Logics

B. Möller **P. Höfner** **G. Struth**

Report 2006-06 June 2006



Institut für Informatik
D-86135 Augsburg

Quantales and Temporal Logics

Bernhard Möller[1], Peter Höfner[1⋆], and Georg Struth[2]

[1] Institut für Informatik, Universität Augsburg
D-86135 Augsburg, Germany
{moeller,hoefner}@informatik.uni-augsburg.de
[2] Department of Computer Science, University of Sheffield
Sheffield S1 4DP, UK
G.Struth@dcs.shef.ac.uk

Abstract We propose an algebraic semantics for the temporal logic CTL* and simplify it for its sublogics CTL and LTL. We abstractly represent state and path formulas over transition systems in Boolean left quantales. These are complete lattices with a multiplication that preserves arbitrary joins in its left argument and is isotone in its right argument. Over these quantales, the semantics of CTL* formulas can be encoded via finite and infinite iteration operators; the CTL and LTL operators can be related to domain operators. This yields interesting new connections between representations as known from the modal μ-calculus and Kleene/ω-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 rarely finds algebraic treatments of their semantics. First results along these lines were obtained by von Karger and Berghammer [23,24]. But the semantic operators involved were characterised only implicitly. For LTL compact closed expressions could be obtained by Desharnais, Möller and Struth in [5] and, in the framework of fork algebras, by Frías and Lopez Pombo [10].

In the present paper we provide compact closed semantic expressions for CTL and LTL by using modal operators in combination with finite and infinite iteration. This is achieved in two steps. First we provide an algebraic semantics for the more expressive logic CTL* on the basis of quantales, i.e., complete lattices with an operation of multiplication that preserves arbitrary joins in its left and non-empty joins in its right argument. In quantales, sets of states and hence the semantics of state formulas can be represented as test elements in the sense of Kozen [15], while general elements represent the semantics of path formulas.

We define suitable mappings that, for the CTL and LTL formulas, transform their general CTL* semantics into simplified versions in ω-regular form. This yields interesting new connections between representations as known from the modal μ-calculus [12] and Kleene/ω-algebra. Our reasoning is purely semantical;

⋆ This research was partially supported by DFG (German Research Foundation)

we do not intend to provide something like an interpretation between logical theories.

The remainder of this paper is organised as follows. Section 2 briefly recapitulates the standard semantics of CTL^* and gives a set-based view of it that prepares the algebraic semantics. In Section 3 we present the algebraic framework of quantales enriched by tests, modal operators and iteration. Section 4 gives an algebraic semantics of full CTL^* that abstracts a set-based view of the standard semantics. The next section discusses the algebraic properties of the semantic element that models the next-time operator. Section 6 shows that the denotations of state formulas are in one-to-one correspondence with tests, i.e., abstract representations of sets of states. This prepares the simplified semantics for CTL and LTL that are derived from the full semantics in Sections 7 and 8. It turns out that much weaker requirements on the underlying algebras now suffice: modal Kleene algebra with a convergence operator in the case of CTL and plain modal Kleene algebra for LTL. A brief conclusion is presented in Section 9.

2 Modelling CTL^*

The language Ψ of *CTL^* formulas* (see e.g. [9]) over a set Φ of atomic propositions is defined by the grammar

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

where X and U are the next-time and until operators and E is the existential quantifier on paths. The logical connectives $\neg, \wedge, \vee, \mathsf{A}$ are defined, as usual, by $\neg\varphi =_{df} \varphi \to \bot$, $\varphi\wedge\psi =_{df} \neg(\varphi \to \neg\psi)$, $\varphi\vee\psi =_{df} \neg\varphi \to \psi$ and $\mathsf{A}\varphi =_{df} \neg\,\mathsf{E}\neg\varphi$. The sublanguages Σ of *state formulas* that denote sets of computation traces and Π of *path formulas* that denote sets of states are given by

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

To motivate our algebraic semantics, we briefly recapitulate the standard CTL^* semantics formulas. Its basic objects are traces σ from S^+ or S^ω, the sets of finite non-empty or infinite words over some set S 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.

Each atomic proposition $\pi \in \Phi$ is associated with the set $S_\pi \subseteq S$ of states for which π is true. The relation $\sigma \models \varphi$ of *satisfaction* of a formula φ by a trace is defined inductively (see e.g. [9]) by

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

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

From this semantics one can extract a set-based one by assigning to each formula φ the set $[\![\varphi]\!] =_{df} \{\sigma \mid \sigma \models \varphi\}$ of paths that satisfy it. This is the basis of the algebraic semantics in Section 4.

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 Section 4:

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

3 Quantales, Modal Operators and Iteration

W now prepare the algebraic setting. A *left quantale* is a structure $(S, \leq, 0, \cdot, 1)$ where $(S, \leq)$ is a complete lattice with least element 0 and an associative multiplication (to model sequential composition) that preserves arbitrary joins in its left and non-empty joins in its right argument. Moreover, 1 is required to be neutral w.r.t. multiplication, playing the role of inaction. The meet and join of two elements $a, b \in S$ are denoted by $a \sqcap b$ and $a + b$, resp. Both operators have equal binding power, which is lower than that of multiplication. The greatest element of S is denoted by $\top$. The definition implies that $\cdot$ is *left-strict*, i.e., that $0 \cdot a = 0$ for all $a \in S$.

A *right quantale* is defined symmetrically. Finally, $(S, \leq, 0, \cdot, 1)$ is a *quantale* [20] if it is both a left and right one. In a (right) quantale multiplication is right-strict, i.e., $a \cdot 0 = 0$ for all $a \in S$. The notion of a quantale is equivalent to that of a *standard Kleene algebra* [3].

A (left) quantale is called *Boolean* if its underlying lattice is distributive and complemented, whence a Boolean algebra. An important Boolean quantale is REL(M), the algebra of binary relations over a set M under set union and relational composition; further examples will be presented below.

General quantale elements abstractly represent sets of paths, i.e., the semantics of path formulas. To model state formulas we use tests as introduced into Kleene algebras by Kozen [15]. In REL(M) a set of elements can be modelled as a subset of the identity relation; meet and join of such partial identities coincide with their composition and union. Generalising this, a *test* in a (left) quantale is an element $p \leq 1$ that has a complement q relative to 1, i.e., $p + q = 1$ and $p \cdot q = 0 = q \cdot p$. The set of all tests of a quantale S is denoted by $\mathsf{test}(S)$. It is not hard to show that $\mathsf{test}(S)$ is closed under $+$ and $\cdot$ and has 0 and 1 as its least and greatest elements. Moreover, the complement $\neg p$ of a test p is uniquely determined. Hence $\mathsf{test}(S)$ forms a Boolean algebra. If S itself is Boolean then $\mathsf{test}(S)$ coincides with the set of all elements below 1. We will consistently write $a, b, c \ldots$ for arbitrary semiring elements and $p, q, r, \ldots$ for tests. Also, we will freely use the standard Boolean operations on $\mathsf{test}(S)$, for instance implication $p \rightarrow q = \neg p + q$, with their usual laws.

With the above definition of tests we deviate slightly from [15], in that we do not allow an arbitrary Boolean algebra of subidentities as $\mathsf{test}(S)$ but only the maximal complemented one. The reason is that the axiomatisation of domain to be presented below will force this maximality anyway (see [6]).

A set of states will now be represented abstractly by a test. Left and right multiplication by a test correspond to restricting an element on the input and output side, resp. This allows us to represent the set of all possible paths that start with a state in set p by the *test ideal* $p \cdot \top$.

Example 3.1 We now introduce two further important Boolean left test quantales. Both are based on finite and infinite words over an alphabet A. Next to their classical interpretation as characters, the elements of A may e.g. be interpreted as states in a computation system, or, in connection with graph algorithms, as nodes in a graph. So words over A can be used to model paths in a transition system. As usual, A^* is the set of all finite words over A including the empty word ε. Moreover, A^ω is the set of all infinite words over A. We set $A^\infty =_{df} A^* \cup A^\omega$. Concatenation is denoted by juxtaposition, where $st =_{df} s$ if $s \in A^\omega$.

A *language* over A is a subset of A^∞. As usual, we identify a singleton language with its only element. For a language $U \subseteq A^\infty$ we define its infinite and finite parts by

$$\mathsf{inf}\, U =_{df} U \cap A^\omega, \qquad \mathsf{fin}\, U =_{df} U - \mathsf{inf}\, U \ .$$

The left Boolean quantale $\mathrm{WOR}(A) = (\mathcal{P}(A^\infty), \subseteq, \emptyset, \cdot, \{\varepsilon\})$ is obtained by extending concatenation to languages in the following way:

$$U \cdot V =_{df} \mathsf{inf}\, U \cup (\mathsf{fin}\, U)\, V \ .$$

Note that in general $U \cdot V \neq ST$; for $V = \emptyset$ one has $ST = \emptyset$, whereas $U \cdot V = \mathsf{inf}\, U$. It is straightforward to show that $\mathrm{WOR}(A)$ is indeed a left quantale. This algebra is well-known from the classical theory of ω-languages (see e.g. [22] for a survey). However, its neutral element is $\{\varepsilon\}$ and therefore its test algebra $\mathsf{test}(\mathrm{WOR}(A)) = \{\emptyset, \{\varepsilon\}\}$ is rather trivial and not suitable for our purposes.

Therefore, besides this model we use a second one with a more refined view of multiplication and hence a richer and more useful test algebra. It uses non-empty words and the *fusion product* $\bowtie$ of words as a language-valued multiplication operation. For $s \in A^+$, $t \in A^\omega$, $u \in A^\infty - \varepsilon$ and $x, y \in A$,

$$sx \bowtie xu =_{df} sxu \ , \qquad sx \bowtie yu =_{df} \emptyset \quad \text{if } x \neq y \ , \qquad t \bowtie u =_{df} t \ .$$

Informally, a finite non-empty word s can be fused with a non-empty word t iff the last letter of s coincides with the first one of t; only one copy of that letter is kept in the fused word.

Since we view the infinite words as streams of computations, we call the left Boolean quantale based on this multiplication operation $\mathrm{STR}(A)$ and define it

by $\mathrm{STR}(A) =_{df} (\mathcal{P}(A^\infty - \varepsilon), \subseteq, \emptyset, \bowtie, A)$, where $\bowtie$ is extended to languages in the following way:

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

This operation has the language A as its neutral element. Moreover, as above, we have $U \bowtie \emptyset = \mathsf{inf}\, U$ and hence $U \bowtie \emptyset = \emptyset$ iff $\mathsf{inf}\, U = \emptyset$. A transition relation over a state set A can be modelled in $\mathrm{STR}(A)$ as a set R of words of length 2. The powers R^i of R then consist of the words (or paths) of length $i+1$ that are generated by R-transitions.

The multiplicative identity A has exactly the subsets of A as its subobjects, so that in this quantale the tests faithfully represent sets of states. □

Over a left Boolean quantale S the *domain operation* $\ulcorner \_ : S \to \mathsf{test}(S)$ returns, for a set of paths represented by an element $a \in S$, the set of their starting states. It is axiomatised by the Galois connection

$$\ulcorner a \leq p \Leftrightarrow a \leq p \cdot \top .$$

This is well defined, since in a Boolean left quantale $\cdot$ preserves arbitrary meets of tests in its left argument [4], and hence in left Boolean quantales domain always exists. By general properties of Galois connections, domain preserves arbitrary joins. For further domain properties see [6].

We list a number of important properties of tests, test ideals and domain; for the proofs see [17].

Lemma 3.2 *Assume a left Boolean quantale.*

(a) $\ulcorner(p \cdot \top) = p$.
(b) $p \leq q \Leftrightarrow p \cdot \top \leq q \cdot \top$.
(c) *If the meet* $a \sqcap b$ *exists then* $p \cdot a \sqcap b = p \cdot (a \sqcap b)$.
Hence also $p \cdot \top \sqcap a = p \cdot a$ *and* $p \cdot (a \sqcap b) = p \cdot a \sqcap p \cdot b$.
(d) $p \cdot a \sqcap q \cdot a = p \cdot q \cdot a$.
(e) $\neg p \cdot \top = \overline{p \cdot \top}$.

By (b) the set of test ideals is isomorphic to the set of tests. To use the above properties freely, we assume for the remainder that S is a Boolean left quantale.

Using domain we define (forward) modal operators. For $a \in S$, $q \in \mathsf{test}(S)$,

$$\langle a \rangle q =_{df} \ulcorner(a \cdot q) , \qquad [a]q =_{df} \neg\langle a \rangle \neg q .$$

The diamond is an abstract inverse-image operator, whereas box generalises the notion of the weakest liberal precondition wlp to Boolean left quantales. If we view a as the transition relation of a command then the test $[a]q$ characterises those states from which no transition under a is possible or the execution of a is guaranteed to end up in a final state that satisfies test q. Both operators are isotone in their test argument. Hence in a Boolean quantale we have the full power of the modal μ-calculus [12] available.

In particular, the *convergence* $\triangle a \in \mathsf{test}(S)$ of an element a, defined by

$$\triangle a \;=_{df}\; \mu x \,.\, [a]x \;,$$

characterises the set of states from which no infinite transition paths emerge.

To make the modal operators well-behaved w.r.t. composition we need to assume that the underlying quantale satisfies

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

since then $\langle a \cdot b \rangle \;=\; \langle a \rangle \circ \langle b \rangle$ and $[a \cdot b] \;=\; [a] \circ [b]$, where $\circ$ is composition of modal operators. Therefore we call a (left) quantale with this property *modal*. Both $\mathrm{WOR}(A)$ and $\mathrm{STR}(A)$ are modal.

We will also need finite iteration a^* and infinite iteration a^ω of quantale elements. They are defined as usual by

$$a^* \;=_{df}\; \mu x \,.\, 1 + a \cdot x \;, \qquad\qquad a^\omega \;=_{df}\; \nu x \,.\, a \cdot x \;,$$

where μ and ν are the least and greatest fixpoint operators, resp. If, like in a Boolean quantale, $+$ is completely conjunctive then, as shown in [1], these operations satisfy the axioms of a left Kleene/ω-algebra [14,2]. The two operations are connected as follows (see e.g. [1]):

$$a^* \cdot b \;=\; \mu x \,.\, b + a \cdot x \;, \qquad\qquad a^\omega + a^* \cdot b \;=\; \nu x \,.\, b + a \cdot x \;. \tag{3}$$

In a modal left quantale, star, convergence and box interact according to the following induction and coinduction laws [6,7]:

$$x \leq p \cdot [a]x \Rightarrow x \leq [a^*]p, \tag{4}$$

$$\triangle a \cdot [a^*]p \;=\; \mu x \,.\, p \cdot [a]x. \tag{5}$$

Dual laws hold for the diamond operator.

Modal quantales (and, more generally, modal ω/convergence algebras) offer additional flexibility compared to PDL [12] and the μ-calculus, since the modal operators are defined for ω-regular expressions, not only for atomic actions.

4 Algebraic Semantics of CTL*

We now give our algebraic interpretation of CTL^* over a Boolean modal quantale S. To save some notation we set $\Phi = \mathsf{test}(S)$. Moreover, we fix an element n (n standing for "next") that represents the transition system underlying the logic. The precise requirements for n will be discussed in Section 5. Then the concrete semantics above generalises to a function $[\![\_]\!] : \Psi \;\to\; S$, where $[\![\varphi]\!]$ abstractly represents the set of paths satisfying formula φ:

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

Using these definitions, it is straightforward to check that

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

Given a set A of states, over the left quantale $\mathrm{STR}(A)$ (see Example 3.1) this semantics coincides with that of Section 2. Another important check of the adequacy of our definitions is provided by the following theorem. The restriction on n mentioned in the assumption will be discussed in the next section.

Theorem 4.1 *Assume that left multiplication with* n *distributes through meets. Then the element* $[\![\varphi \,\mathsf{U}\, \psi]\!]$ *is the least fixpoint* μf *of the function* $f(y) =_{df} [\![\psi]\!] + ([\![\varphi]\!] \sqcap \mathsf{n} \cdot y)$.

Proof. Since in a Boolean quantale multiplication and binary meet preserve arbitrary joins, f preserves arbitrary joins, too, and hence is continuous. So by Kleene's fixpoint theorem $\mu f = \bigsqcup_{j \geq 0} f^j(0)$. A straightforward induction shows that

$$f^i(0) = \bigsqcup_{j \leq i} (\mathsf{n}^j \cdot [\![\psi]\!] \sqcap \bigsqcap_{k<j} \mathsf{n}^k \cdot [\![\varphi]\!]),$$

from which the claim is immediate. □

We define the usual abbreviations:

$$\mathsf{A}\varphi \;=_{df}\; \neg\mathsf{E}\neg\varphi, \qquad \mathsf{F}\varphi \;=_{df}\; \top\mathsf{U}\varphi, \qquad \mathsf{G}\varphi \;=_{df}\; \neg\mathsf{F}\neg\varphi.$$

Theorem e4.1 and (3) yield the following closed representation of F:

Corollary 4.2 $[\![\mathsf{F}\varphi]\!] = \mathsf{n}^* \cdot [\![\varphi]\!]$.

5 The Next-Time Operator

We now want to find suitable requirements on n by considering axiom (1) in the algebraic setting. To satisfy it, we need to have for all formulas φ and their semantical values $b =_{df} [\![\varphi]\!]$,

$$\overline{\mathsf{n} \cdot b} = [\![\neg\mathsf{X}\varphi]\!] = [\![\mathsf{X}\neg\varphi]\!] = \mathsf{n} \cdot \overline{b}. \tag{6}$$

This semantic property can equivalently be characterised as follows (property (a) was already shown in [4]).

Lemma 5.1 *Consider a Boolean left quantale* S *and* $\mathsf{n} \in S$ *such that* $\mathsf{n} \cdot 0 = 0$.
(a) $\forall b \in S : \mathsf{n} \cdot \overline{b} \leq \overline{\mathsf{n} \cdot b} \Leftrightarrow \forall b, c \in S : \mathsf{n} \cdot (b \sqcap c) = \mathsf{n} \cdot b \sqcap \mathsf{n} \cdot c$.
(b) $\forall b \in S : \overline{\mathsf{n} \cdot b} \leq \mathsf{n} \cdot \overline{b} \Leftrightarrow \mathsf{n} \cdot \top = \top \Leftrightarrow \mathsf{n}^\omega = \top$.

Proof. (a) ($\Rightarrow$) It suffices to show ($\geq$), since the reverse inequality follows by isotony. By shunting, the assumption $\mathsf{n} \cdot \overline{b} \leq \overline{\mathsf{n} \cdot b}$, distributivity, Boolean algebra, and lattice algebra:

$$\mathsf{n}\cdot b\sqcap \mathsf{n}\cdot c\le \mathsf{n}\cdot(b\sqcap c)\Leftrightarrow \mathsf{n}\cdot b\le \overline{\mathsf{n}\cdot \overline{c}}+\mathsf{n}\cdot(b\sqcap c)\Leftarrow \mathsf{n}\cdot b\le \mathsf{n}\cdot \overline{c}+\mathsf{n}\cdot(b\sqcap c)$$
$$\Leftrightarrow \mathsf{n}\cdot b\le \mathsf{n}\cdot(\overline{c}+(b\sqcap c))\Leftrightarrow \mathsf{n}\cdot b\le \mathsf{n}\cdot(\overline{c}+b)\Leftrightarrow \mathsf{TRUE}.$$

($\Leftarrow$) We calculate, using the assumption in the third step:

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

Now the claim is immediate by shunting.

(b) By shunting, distributivity, complement, greatest element, and $\mathsf{n}^\omega=\nu y\,.\,\mathsf{n}\cdot y$:

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

□

In relation algebra, the special case $\mathsf{n}\cdot\overline{1}\le\overline{\mathsf{n}}$ of the property in (a) characterises n as a partial function and is equivalent to the full property [21]. But in general quantales the special and the general case are not equivalent [4]. Moreover, again from [4], we know that in quantales such as WOR and STR an element n is left-distributive over meet iff it is prefix-free, i.e. if no member of n is a prefix of another member. This holds in particular if all words in n have equal length, which is the case if n models a transition relation and hence consists only of words of length 2. The equivalent condition $\forall b\,.\,\mathsf{n}\cdot b\sqcap\mathsf{n}\cdot\overline{b}=0$ was used in the computation calculus of R.M. Dijkstra [8].

But what about property (b)? Only rarely will a quantale be "generated" by an element n in the sense that $\mathsf{n}^\omega=\top$. The solution is to choose a left-distributive element n and restrict the set of semantical values to the subset $\mathrm{SEM}(\mathsf{n})=_{df}\{b : b\le\mathsf{n}^\omega\}$, taking complements relative to n^ω. This set is clearly closed under $+$ and $\sqcap$ and under prefixing by n, since by isotony

$$\mathsf{n}\cdot b\le \mathsf{n}\cdot\mathsf{n}^\omega=\mathsf{n}^\omega\ .$$

Finally, it also contains all elements $p\cdot\mathsf{n}^\omega$ with $p\in\mathsf{test}(S)$, since $p\le 1$. Hence the above semantics is well-defined in $\mathrm{SEM}(\mathsf{n})$ if we replace $\top$ by n^ω.

6 The Semantics of State Formulas

In this section we show, next to some 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 Section 7.

Theorem 6.1 *Let φ be a state formula of* CTL^*.

(a) $[\![\varphi]\!]$ *is a test ideal, and hence, by Lemma 3.2(a),* $[\![\varphi]\!]=\ulcorner[\![\varphi]\!]\cdot\top$.

(b) $[\![\mathsf{E}\varphi]\!]=[\![\varphi]\!]$.

(c) $[\![\mathsf{A}\varphi]\!]=\neg\ulcorner(\overline{[\![\varphi]\!]})\cdot\top$.

Proof. (a) The proof is by induction on the structure of φ.

– For $\bot$ and $p\in\mathsf{test}(S)$ this is immediate from the definition.

– Assume that the claim already holds for state formulas φ and ψ. We calculate, using the definitions, the induction hypothesis, Lemma 3.2(e), distributivity and the definitions again,

$$\begin{aligned}[\![\varphi \to \psi]\!] &= \overline{[\![\varphi]\!]} + [\![\psi]\!] = \overline{\lceil [\![\varphi]\!] \cdot \top} + \lceil [\![\psi]\!] \cdot \top = \neg \lceil [\![\varphi]\!] \cdot \top + \lceil [\![\psi]\!] \cdot \top \\ &= (\neg \lceil [\![\varphi]\!] + \lceil [\![\psi]\!]) \cdot \top = (\lceil [\![\varphi]\!] \to \lceil [\![\psi]\!]) \cdot \top.\end{aligned}$$

– For $\mathsf{E}\varphi$ the claim is immediate from the definition.

(b) Immediate from (a) and the definition of $[\![\mathsf{E}\varphi]\!]$.

(c) Similar to (b). □

Moreover, state formulas are closed under $\neg, \wedge, \vee$ and A.

Next, we derive some properties of U and its relatives for state formulas. For this we use knowledge about dual functions and their fixpoints. The *(de Morgan) dual* f° of a function $f : S \to S$ over a Boolean quantale is, as usual, defined by $f^\circ(y) =_{df} \overline{f(\overline{y})}$. Then $\mu f = \overline{\nu f^\circ}$ and $\nu f = \overline{\mu f^\circ}$.

Lemma 6.2 *Let φ, ψ be state formulas of CTL^* and $p \cdot \top =_{df} [\![\varphi]\!], q \cdot \top =_{df} [\![\psi]\!]$.*

(a) $[\![\varphi \mathsf{U} \psi]\!] = (p \cdot \mathsf{n})^* \cdot q \cdot \top = ([\![\varphi]\!] \sqcap \mathsf{n})^* \cdot [\![\psi]\!]$.

(b) $[\![\mathsf{G}\varphi]\!] = (p \cdot \mathsf{n})^\omega = ([\![\varphi]\!] \sqcap \mathsf{n})^\omega$.
Hence we have the shunting rule $(p \cdot \mathsf{n})^\omega = \overline{\mathsf{n}^* \cdot \neg p \cdot \top}$.

Proof. (a) Using Theorem 4.1 and Lemma 3.2(c) 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 (3).

(b) Since $[\![\mathsf{F}\varphi]\!] = \mu f_p$ where $f_p(y) = p \cdot \top + \mathsf{n} \cdot y$, we have, by Lemma 3.2(e), $[\![\mathsf{G}\varphi]\!] = [\![\neg \mathsf{F} \neg \varphi]\!] = \nu f^\circ_{\neg p}$, where, again by Lemma 3.2(e) and by (6),

$$f^\circ_{\neg p}(y) = \overline{\neg p \cdot \top + \mathsf{n} \cdot \overline{y}} = \overline{\neg p \cdot \top} \sqcap \overline{\mathsf{n} \cdot \overline{y}} = p \cdot \top \sqcap \mathsf{n} \cdot y = p \cdot \mathsf{n} \cdot y.$$

Hence the claim follows by the definition of ω. □

The case $p = 1$ yields again Corollary 4.2. Now we deal with E.

Lemma 6.3 $[\![\mathsf{EX}\varphi]\!] = [\![\mathsf{EXE}\varphi]\!]$.

Proof. By the definitions, properties of domain, (2) and the definitions again,

$$[\![\mathsf{EXE}\varphi]\!] = \lceil (\mathsf{n} \cdot \lceil [\![\varphi]\!] \cdot \top) \cdot \top = \lceil (\mathsf{n} \cdot \lceil [\![\varphi]\!]) \cdot \top = \lceil (\mathsf{n} \cdot [\![\varphi]\!]) \cdot \top = [\![\mathsf{EX}\varphi]\!]. \quad \square$$

Next, we collect a number of properties of A. The proofs are straightforward calculations.

Lemma 6.4 *For atomic proposition $p \in \mathsf{test}(S)$,*

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

Moreover, for the axiom $\mathsf{EX}\top$ we obtain

Lemma 6.5 $[\![\mathsf{EX}\top]\!] = \top \Leftrightarrow \ulcorner \mathsf{n} = 1 \Leftrightarrow \mathsf{n}$ *total.*

Proof. This follows by Lemma 3.2(b), since $[\![\mathsf{EX}\top]\!] = \ulcorner(\mathsf{n} \cdot \top) \cdot \top = \ulcorner \mathsf{n} \cdot \top$. □

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

Lemma 6.6 $[\![\mathsf{AX}\varphi]\!] = [\![\neg\mathsf{EX}\neg\varphi]\!]$.

From this and Lemma 6.3 we obtain

Corollary 6.7 $[\![\mathsf{AX}\varphi]\!] = [\![\mathsf{AXA}\varphi]\!]$.

7 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/convergence algebra. Syntactically, CTL consists of those CTL^* state formulas that only use path formulas of the restricted form $\Pi ::= \mathsf{X}\Sigma \mid \Sigma\,\mathsf{U}\Sigma$.

From the previous section we already know that the semantics of every CTL formula is a test ideal t, from which, by Theorem 6.1(a), we can extract the corresponding test (or state set) as $\ulcorner t$. This is reflected by the simplified semantics

$$[\![\varphi]\!]_d =_{df} \ulcorner[\![\varphi]\!].$$

This enables us to calculate solely with tests.

First, for the Boolean connectives we obtain by disjunctivity of domain and Lemma 3.2,

$$[\![\varphi \vee \psi]\!]_d = [\![\varphi]\!]_d + [\![\psi]\!]_d, \qquad [\![\varphi \wedge \psi]\!]_d = [\![\varphi]\!]_d \cdot [\![\psi]\!]_d, \qquad [\![\neg\varphi]\!]_d = \neg[\![\varphi]\!]_d.$$

Next, we transfer the properties of A from Lemma 6.4 to the simplified semantics. Again the proofs are straightforward calculations.

Lemma 7.1 *For atomic proposition* $p \in \mathsf{test}(S)$,

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

Now we can calculate the inductive behaviour of $[\![\_]\!]_d$ for all CTL formulas.

Theorem 7.2

(a) $[\![\bot]\!]_d = 0$,
(b) $[\![p]\!]_d = p$,
(c) $[\![\varphi \to \psi]\!]_d = [\![\varphi]\!]_d \to [\![\psi]\!]_d$,
(d) $[\![\mathsf{EX}\varphi]\!]_d = \langle \mathsf{n} \rangle [\![\varphi]\!]_d$,
(e) $[\![\mathsf{AX}\varphi]\!]_d = [\mathsf{n}][\![\varphi]\!]_d = [\![\mathsf{AXA}\varphi]\!]_d$,
(f) $[\![\mathsf{AF}\varphi]\!]_d = \neg\overline{\ulcorner \mathsf{n}^* \cdot [\![\varphi]\!]_d \cdot \top} = \neg\ulcorner(\neg[\![\varphi]\!]_d \cdot \mathsf{n})^\omega$,
(g) $[\![\mathsf{E}(\varphi\mathsf{U}\psi)]\!]_d = \langle([\![\varphi]\!]_d \cdot \mathsf{n})^* \rangle [\![\psi]\!]_d$,
(h) $[\![\mathsf{A}(\varphi\mathsf{U}\psi)]\!]_d = [\![A\mathsf{F}\varphi]\!]_d \cdot [b^*]([\![\varphi]\!]_d + [\![\psi]\!]_d)$ *where* $b =_{df} \neg[\![\varphi]\!]_d \cdot \mathsf{n}$.

The lengthy proof by induction on the structure of the state formulas can be found in the Appendix. This theorem 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 [17] is sufficient.

To complete the picture, we show the validity of the usual least-fixpoint characterisation of $\mathsf{A}(u)$, where $u = [\![\varphi \mathsf{U} \psi]\!]$ for state formulas φ and ψ. Then, by Lemma 4.1, the definition of f, Lemma 6.4 twice and Corollary 6.7, we obtain

$$\mathsf{A}(u) = \mathsf{A}(f(u)) = \mathsf{A}(q \cdot \top + p \cdot \mathsf{n} \cdot u) = q \cdot \top + p \cdot \mathsf{A}(\mathsf{n} \cdot u) = q \cdot \top + p \cdot \mathsf{A}(\mathsf{n} \cdot \mathsf{A}(u)).$$

In general quantales, however, $\mathsf{A}(u)$ need not be the least fixpoint of the associated function. We need an additional assumption on the underlying quantale S, namely that unlimited finite iteration can be extended to infinite iteration in the following sense:

$$\forall\, b \in S : \bigsqcap_{i \in \mathbb{N}} \lceil(b^i) \leq \lceil(b^\omega). \tag{7}$$

In particular, S must have "enough" infinite elements to make $b^\omega \neq 0$ if all $b^i \neq 0$. This property is violated in the subquantale LAN of WOR in which only languages of finite words are allowed, because in LAN finite languages may be iterated indefinitely, but no infinite "limits" exist.

Now we can show the desired leastness of A.

Theorem 7.3 *Assume (7).*

(a) $\neg\lceil(b^\omega) = \triangle b$.
(b) *If b is total, i.e., $\lceil b = 1$ then also $\lceil(b^\omega) = 1$.*
(c) *If $[\![\varphi]\!] = p \cdot \top$ then $[\![\mathsf{AF}\varphi]\!]_d = \triangle\neg p \cdot \mathsf{n}$.*
(d) $[\![\varphi \mathsf{U} \psi]\!]_d = \mu h$, *where* $h(y) =_{df} q + p \cdot [\mathsf{n}]y$.

Proof. (a) First, $\neg\lceil(b^\omega)$ is a fixpoint of $[b]$:

$$\neg\lceil(b^\omega) = \neg\lceil(b \cdot (b^\omega)) = \neg\lceil(b \cdot \neg\neg(b^\omega)) = [b](\neg\lceil(b^\omega)).$$

Hence $\triangle b = \mu[b] \leq \neg\lceil(b^\omega)$. For the converse inequation we calculate By shunting, (7), and the definition of meet:

$$\neg\lceil(b^\omega) \leq \triangle b \Leftrightarrow \neg\triangle b \leq \lceil(b^\omega) \Leftarrow \neg\triangle b \leq \bigsqcap_{i \in \mathbb{N}} \lceil(b^i) \Leftarrow \forall\, i \in \mathbb{N} : \neg\triangle b \leq \lceil(b^i).$$

Using $\neg\triangle b \leq 1$, isotony of domain, the definition of box and that $\triangle b$ is a fixpoint of $[b]$, we have indeed $\lceil(b^i) \geq \lceil(b^i \cdot \neg\triangle b) = \neg[b^i]\triangle b = \neg\triangle b$.

(b) By the assumption (2) of modality multiplication preserves totality: if $\lceil a = \lceil b = 1$ then $\lceil(a \cdot b) = \lceil(a \cdot \lceil b) = \lceil(a \cdot 1) = \lceil a = 1$. Now an easy induction shows $\lceil b = 1 \Rightarrow \forall\, i : \lceil b^i = 1$ and assumption (7) immediately implies the claim.
(c) Immediate from Theorem 7.2(f) and (a).
(d) From the definition of h we get by Boolean algebra

$$h(y) = (q + p) \cdot (q + [\mathsf{n}]y).$$

Now the claim follows from (5), Theorem 7.2(h) and (b). □

This result shows that for CTL we can even do without omega iteration and need only a convergence algebra. Recently it has been shown [13] that property (a) is equivalent to validity of the coinduction rule

$$p \leq \ulcorner(q + a \cdot p) \Rightarrow p \leq \ulcorner(a^\omega + a^* \cdot q) \ .$$

8 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, the LTL path formulas are given by

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

The LTL semantics is embedded into the CTL* one by assigning to $\varphi \in \Pi$ the semantic value $[\![\mathsf{A}\varphi]\!]$.

Unfortunately, except for the cases $[\![\mathsf{AX}\varphi]\!] = [\mathsf{n}][\![\mathsf{A}\varphi]\!]$ and $[\![\mathsf{AG}\varphi]\!] = [\mathsf{n}^*][\![\mathsf{A}\varphi]\!]$ the semantics does not propagate nicely in an inductive way into the subformulas, and so a simplified semantics cannot be obtained directly from the CTL* one.

However, by a slight change of view we can still achieve our goal. In the considerations based on the concrete quantales WOR and STR, the semantic element n representing X "glued" transitions to the front of traces. However, as is frequently done, one can also interpret n as a relation that maps a trace σ to its tail σ^1. This is the basis for a simplified semantics of LTL over the Boolean quantale $\mathrm{REL}(\mathrm{A}^\omega)$ (since standard LTL considers only infinite traces) for some set A of states.

What are the tests involved? Obviously, they now correspond to sets of paths, since they are subrelations of the identity relation on traces. So in this view the semantics of LTL formulas is again given by test ideals, only in a different algebra.

Therefore we can re-use the simplified CTL semantics. In particular, we set

$$[\![\mathsf{X}\varphi]\!]_{\mathsf{L}} \ =_{df} \ \langle \mathsf{n} \rangle [\![\varphi]\!]_{\mathsf{L}}.$$

This means that $[\![\mathsf{X}\varphi]\!]_{\mathsf{L}}$ is the inverse image of $[\![\varphi]\!]_{\mathsf{L}}$ under the tail relation; hence the standard LTL semantics is captured faithfully.

What does axiom (1) mean in this interpretation? It is equivalent to the equation $\langle \mathsf{n} \rangle = [\mathsf{n}]$ which characterises $\langle \mathsf{n} \rangle$ as a total function. This holds indeed for the tail relation on A^ω.

The semantics of $\bot$ and $\to$ are as before. It remains to work out the semantics of U. With $p =_{df} [\![\varphi]\!]_{\mathsf{L}}$ and $q =_{df} [\![\psi]\!]_{\mathsf{L}}$, we want $[\![\varphi \mathsf{U} \psi]\!]_{\mathsf{L}}$ to be the least fixpoint of the function $h(y) =_{df} q + p \cdot \langle \mathsf{n} \rangle y$, which by the dual of box induction (5) is $\langle (p \cdot \mathsf{n})^* \rangle q$. By this, the semantics of $\mathsf{F}\psi$ and $\mathsf{G}\psi$ work out to $\langle \mathsf{n}^* \rangle q$ and $[\mathsf{n}^*]q$.

Summarising, our LTL semantics now reads (see also [5])

$$\begin{aligned}
[\![\bot]\!]_{\mathsf{L}} &= 0,\\
[\![p]\!]_{\mathsf{L}} &= p,\\
[\![\varphi \to \psi]\!]_{\mathsf{L}} &= [\![\varphi]\!]_{\mathsf{L}} \to [\![\psi]\!]_{\mathsf{L}},\\
[\![\mathsf{X}\varphi]\!]_{\mathsf{L}} &= \langle \mathsf{n} \rangle [\![\varphi]\!]_{\mathsf{L}},\\
[\![\varphi \,\mathsf{U}\, \psi]\!]_{\mathsf{L}} &= \langle ([\![\varphi]\!]_{\mathsf{L}} \cdot \mathsf{n})^* \rangle [\![\psi]\!]_{\mathsf{L}},\\
[\![\mathsf{F}\psi]\!]_{\mathsf{L}} &= \langle \mathsf{n}^* \rangle [\![\psi]\!]_{\mathsf{L}},\\
[\![\mathsf{G}\psi]\!]_{\mathsf{L}} &= [\mathsf{n}^*] [\![\psi]\!]_{\mathsf{L}}.
\end{aligned}$$

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.

9 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 or the convergence operator. 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 a modal omega or convergence algebra an even just a modal Kleene algebra, resp.

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 [16] seem a promising candidate.

Acknowledgements We are grateful to the anonymous referees and to Kim Solin for valuable comments and remarks.

References

1. R. C. Backhouse et al.: Fixed point calculus. Inform. Proc. Letters, 53:131–136 (1995)
2. E. Cohen: Separation and reduction. In R. Backhouse and J.N. Oliveira (eds.): Mathematics of Program Construction. LNCS 1837. Springer 2000, 45–59
3. J.H. Conway: Regular algebra and finite machines. London: Chapman and Hall 1971
4. J. Desharnais, B. Möller: Characterizing determinacy in Kleene algebra. Special Issue on Relational Methods in Computer Science, Information Sciences — An International Journal 139, 253–273 (2001)
5. J. Desharnais, B. Möller, G. Struth: Modal Kleene algebra and applications — a survey. J. Relational Methods in Computer Science 1, 93–131 (2004)

6. J. Desharnais, B. Möller, G. Struth: Kleene algebra with domain. ACM Transactions on Computational Logic 2006 (to appear)
7. J. Desharnais, B. Möller, G. Struth: Termination in modal Kleene algebra. In J.-J. Lévy, E. Mayr, and J. Mitchell, editors, Exploring new frontiers of theoretical informatics. IFIP International Federation for Information Processing Series 155. Kluwer 2004, 653–666
8. R.M. Dijkstra: Computation calculus bridging a formalisation gap. Science of Computer Programming **37**, 3-36 (2000)
9. 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
10. M.F. Frías and C. Lopez Pombo. Interpretability of linear time temporal logic in fork algebra. Journal of Logic and Algebraic Programming, 66(2):161-184 (2006)
11. V. Goranko: Temporal logics of computations. Introductory course, 12th European summer School in Logic, Language and Information, Birmingham, 6–18 August 2000
12. D. Harel, D. Kozen, J. Tiuryn: Dynamic Logic. MIT Press 2000
13. P. Höfner, B. Möller, K. Solin: Omega Algebra, Demonic Refinement Algebra and Commands. Institute of Computer Science, University of Augsburg, Technical Report 2006-11, March 2006
14. D. Kozen: A completeness theorem for Kleene algebras and the algebra of regular events. Information and Computation **110:2**, 366–390 (1994)
15. D. Kozen: Kleene algebras with tests. ACM TOPLAS **19**, 427–443 (1997)
16. D. Kozen: Some results in dynamic model theory. Science of Computer Programming 51, 3–22 (2004)
17. B. Möller: Kleene getting lazy. Science of Computer Programming, Special issue on MPC 2004 (to appear). Previous version: B. Möller: Lazy Kleene algebra. In D. Kozen (ed.): Mathematics of program construction. LNCS 3125. Springer 2004, 252–273
18. B. Möller, G. Struth: Algebras of Modal Operators and Partial Correctness Theoretical Computer Science 351, 221-239 (2006)
19. B. Möller, G. Struth: wp is wlp. In W. MacCaull, M. Winter and I. Düntsch (eds.): Relational Methods in Computer Science. LNCS 3929. Springer 2006 (in press)
20. K.I. Rosenthal: Quantales and their applications. Pitman Research Notes in Mathematics Series, Vol. 234. Longman Scientific&Technical 1990
21. G. Schmidt, T. Ströhlein: Relations and Graphs — Discrete Mathematics for Computer Scientists. EATCS Monographs on Theoretical Computer Science. Springer 1993
22. L. Staiger: Omega languages. In G. Rozenberg, A. Salomaa (eds.): Handbook of formal languages, Vol. 3. Springer 1997, 339–387
23. B. von Karger: Temporal algebra. Mathematical Structures in Computer Science 8:277–320, 1998
24. B. von Karger, R. Berghammer: A relational model for temporal logic. Logic Journal of the IGPL 6, 157–173, 1998

Appendix: Proof of Theorem 7.2

The proof is again by induction on the structure of the state formulas. The cases (a)–(c) of $\bot$, p and $\varphi \to \psi$ have already been covered in the proof of Theorem 6.1.

(d) Using again Theorem 6.1, the definition of $[\![\ ]\!]$, (2) and the definitions again, we calculate $[\![\mathsf{EX}\varphi]\!]_d = \lceil [\![\mathsf{X}\varphi]\!] = \lceil(\mathsf{n} \cdot [\![\varphi]\!]) = \lceil(\mathsf{n} \cdot \lceil [\![\varphi]\!]) = \langle \mathsf{n} \rangle [\![\varphi]\!]_d$.

(e) By Theorem 6.1(c) and Lemma 3.2(b), definition and Theorem 6.1, by (6), by Lemma 3.2(b), domain property, and the definition:

$$[\![\mathsf{AX}\varphi]\!]_d = \neg\lceil\overline{[\![\mathsf{X}\varphi]\!]} = \neg\lceil\overline{\mathsf{n} \cdot [\![\varphi]\!]_d \cdot \top} = \neg\lceil(\mathsf{n} \cdot \overline{[\![\varphi]\!]_d \cdot \top}) = \neg\lceil(\mathsf{n} \cdot \neg[\![\varphi]\!]_d \cdot \top) = \neg\lceil(\mathsf{n} \cdot \neg[\![\varphi]\!]_d) = [\mathsf{n}][\![\varphi]\!]_d.$$

Moreover, $[\![\varphi]\!]_d = [\![\mathsf{A}\varphi]\!]_d$ follows from Lemma 7.1.

(f) Assume $[\![\varphi]\!] = p \cdot \top$. By the definition of A and the explicit representation of F from Corollary 4.2 we obtain $[\![\mathsf{AF}\varphi]\!] = \neg\lceil\overline{\mathsf{n}^* \cdot p \cdot \top} \cdot \top$. Now the claim follows from the shunting rule of Lemma 6.2(b) and the definition of $[\![\ ]\!]_d$.

(g) For $[\![\mathsf{E}(\varphi \mathsf{U} \psi)]\!]$ we use the principle of *least-fixpoint fusion* [1]: If h preserves arbitrary joins and $h \circ f = g \circ h$ then $h(\mu f) = \mu g$.
Set, for abbreviation, $p =_{df} [\![\varphi]\!]_d$ and $q =_{df} [\![\psi]\!]_d$. Then, by Lemma 4.1 and Lemma 3.2(c), $u =_{df} [\![\varphi \mathsf{U} \psi]\!] = \mu f$ where $f(y) =_{df} q \cdot \top + (p \cdot \mathsf{n} \cdot y)$. Second, by Theorem 6.1 and (5), $\langle (p \cdot \mathsf{n})^* \rangle = \mu g$ where $g(p) =_{df} q + \langle (p \cdot \mathsf{n}) \rangle p$. We need to show $\lceil(\mu f) = \mu g$. By the principle of least-fixpoint fusion this is implied by $\lceil \circ f = g \circ \lceil$, since $\lceil$ preserves arbitrary joins. We calculate: By definition f, additivity of domain, Lemma 3.2(a), by (2), definition diamond, and definition g:

$$\lceil(f(y)) = \lceil(q \cdot \top + (p \cdot \mathsf{n} \cdot y)) = \lceil(q \cdot \top) + \lceil(p \cdot \mathsf{n} \cdot y)) = q + \lceil(p \cdot \mathsf{n} \cdot y) = q + \lceil(p \cdot \mathsf{n} \cdot \lceil y) = q + \langle p \cdot \mathsf{n} \rangle \cdot \lceil y = g(\lceil y).$$

(h) For $r =_{df} [\![\mathsf{A}(\varphi \mathsf{U} \psi)]\!]$ we use that, by Theorem 6.1(c), $r = \neg\lceil\overline{u}$, where $u =_{df} [\![\varphi \mathsf{U} \psi]\!]$. Let, for abbreviation, $p \cdot \top =_{df} [\![\varphi]\!]$ and $q \cdot \top =_{df} [\![\psi]\!]$. Since $u = \mu f$ where $f(y) = q \cdot \top + p \cdot \mathsf{n} \cdot y$, we have $\overline{u} = \nu f^\circ$. By the definitions, de Morgan, Lemma 3.2(e), Lemma 3.2(c) and de Morgan, Lemma 3.2(e) and (6), complement, distributivity, and de Morgan:

$$f^\circ(y) = \overline{q \cdot \top + p \cdot \mathsf{n} \cdot \overline{y}} = \overline{q \cdot \top} \sqcap \overline{p \cdot \mathsf{n} \cdot \overline{y}} = \neg q \cdot \top \sqcap \overline{p \cdot \top \sqcap \mathsf{n} \cdot \overline{y}}$$
$$= \neg q \cdot (\overline{p \cdot \top} + \overline{\mathsf{n} \cdot \overline{y}}) = \neg q \cdot (\neg p \cdot \top + \overline{\overline{\mathsf{n} \cdot y}}) = \neg q \cdot (\neg p \cdot \top + \mathsf{n} \cdot y)$$
$$= \neg q \cdot \neg p \cdot \top + \neg q \cdot \mathsf{n} \cdot y = \neg(p + q) \cdot \top + \neg q \cdot \mathsf{n} \cdot y.$$

By the above, (3), distributivity and de Morgan, Lemma 6.2 (b) and a domain property, Theorem 6.1(c) and definition of box, and Lemma 4.2:

$$\begin{aligned}
& r \\
= \ & \neg\lceil(\nu f^\circ) \\
= \ & \neg\lceil((\neg q \cdot \mathsf{n})^\omega + (\neg q \cdot \mathsf{n})^* \cdot \neg(p + q) \cdot \top) \\
= \ & \neg\lceil((\neg q \cdot \mathsf{n})^\omega) \cdot \neg\lceil((\neg q \cdot \mathsf{n})^* \cdot \neg(p + q) \cdot \top) \\
= \ & \neg\lceil\overline{(\mathsf{n}^* \cdot q \cdot \top)} \cdot \neg\lceil((\neg q \cdot \mathsf{n})^* \cdot \neg(p + q)) \\
= \ & \mathsf{A}(\mathsf{n}^* \cdot q \cdot \top) \cdot [(\neg q \cdot \mathsf{n})^*](p + q) \\
= \ & (\mathsf{AF}q) \cdot [(\neg q \cdot \mathsf{n})^*](p + q).
\end{aligned}$$