From Linear Temporal Logic Properties to Rewrite Propositions

Pierre-Cyrille Héam*, Vincent Hugot**, and Olga Kouchnarenko

FEMTO-ST CNRS 6174, University of Franche-Comté & INRIA/CASSIS, France
{pierre-cyrille.heam,vincent.hugot,olga.kouchnarenko}@inria.fr

Abstract. In the regular model-checking framework, reachability analysis can be guided by temporal logic properties, for instance to achieve the counter example guided abstraction refinement (CEGAR) objectives. A way to perform this analysis is to translate a temporal logic formula expressed on maximal rewriting words into a "rewrite proposition" – a propositional formula whose atoms are language comparisons, and then to generate semi-decision procedures based on (approximations of) the rewrite proposition. This approach has recently been studied using a non-automatic translation method. The extent to which such a translation can be systematised needs to be investigated, as well as the applicability of approximated methods wherever no exact translation can be effected. This paper presents contributions to that effect: **(1)** we investigate suitable semantics for LTL on maximal rewriting words and their influence on the feasibility of a translation, and **(2)** we propose a general scheme providing exact results on a fragment of LTL corresponding mainly to safety formulæ, and approximations on a larger fragment.

1 Introduction & Context

Term rewriting and rewriting logic have been intensively and successfully used for solving equational problems in automated deduction, for programming language definitions, for model transformations and generation of efficient interpreters as well as for specification and verification in software engineering. In this last context, system states are modelled by languages, while rewrite rules stand for *actions* of the system; for instance procedure or method calls. This technique has been successfully used to prove the security of cryptographic protocols [11] and Java Bytecode programs [3]. When proving security, reachability analysis over sets of terms can be guided by temporal logic properties, like e.g., in [7,6].

In [7], three specific Linear Temporal Logic (LTL) formulæ – chosen for their relevance to model-checking [13], in particular with respect to `Java` MIDLets, in the framework of the French ANR RAVAJ project – have been translated into what we will call *rewrite propositions*, with respect to straightforward semantics

* This author is supported by the project ANR 2010 BLAN 0202 02 FREC.
** This author is supported by the French DGA (Direction Générale de l'Armement).

for LTL on finite words. For instance, given a rewrite system $\mathcal{R}$, of which $X, Y \subseteq \mathcal{R}$ are subsets, and an initial language Π, the LTL property $\Box(X \Rightarrow \bullet Y)$ signifies that whenever an accessible term is rewritten by some rewrite rule in X, then the resulting term can be rewritten by some rule in Y, and not by any other rule. As shown in [7], that property is satisfied if and only if the following rewrite proposition holds: $[\mathcal{R} \setminus Y]\left(X\left(\mathcal{R}^*(\Pi)\right)\right) = \varnothing \wedge X\left(\mathcal{R}^*(\Pi)\right) \subseteq Y^{-1}(\mathcal{T}(\mathbb{A}))$, where $\mathcal{R}^*(\Pi)$ is the transitive-reflexive forward closure of Π by $\mathcal{R}$, and $\mathcal{T}(\mathbb{A})$ is the set of all trees. The point of translating satisfaction in terms of rewrite propositions is that they present a more tractable intermediary form which can itself be translated into automata-based (semi-)decision procedures. Indeed, if the initial language Π is regular, then the literature is rife with constructive results concerning questions such as preservation of regularity under a rewriting step, or under forward closure; that is to say, "under which conditions on the rewrite system $\mathcal{R}$ is $\mathcal{R}(\Pi)$ (resp. $\mathcal{R}^*(\Pi)$) still regular?". And when preserving regularity is not an option, one may fall back on more expressive classes of tree automata (TA) such as TAGED [10]. As an example of both aspects, [7, Prop. 5] states that a language given by $\mathcal{R}^{-1}(\mathcal{T}(\mathbb{A}))$ can in all generality be represented by a positive TAGED; furthermore, if $\mathcal{R}$ is left-linear, then regularity is preserved. Such results can be combined with regular approximation techniques; for instance, if $\mathcal{A}$ is a tree automaton, a procedure $\texttt{Approx}(\mathcal{A}, \mathcal{R})$ in [4] yields another TA $\mathcal{B}$ such that $\mathfrak{Lang}(\mathcal{B}) \supseteq \mathcal{R}^*(\mathfrak{Lang}(\mathcal{A}))$, where $\mathfrak{Lang}(\mathcal{A})$ is the language accepted by $\mathcal{A}$. Put together, those tools provide a framework for building decision and semi-decision procedures from rewrite propositions. For instance, the proposition given above is semi-decided by the conjunction of the procedures $\texttt{IsEmpty}(\texttt{OneStep}(\mathcal{R} \setminus Y, \texttt{Approx}(\mathcal{A}, \mathcal{R})), X)$ and $\texttt{Subset}(\texttt{OneStep}(X, \texttt{Approx}(\mathcal{A}, \mathcal{R})), \texttt{Backward}(Y))$, where $\mathfrak{Lang}(\mathcal{A}) = \Pi$ and under the additional constraint that Y must be left-linear. Note that this is almost a straightforward reformulation of the original rewrite proposition.

To summarise the above, our approach to model-checking temporal properties of sequences of rewrite rules consists of two phases outlined in [7]: **(1)** translation of a temporal logic formula expressed on maximal rewriting words into a "rewrite proposition" – a propositional formula whose atoms are language comparisons, and **(2)** translation of the rewrite proposition into a semi-decision procedure. To make this approach useful for program verification, both steps must be automated; neither is at present. The *general question* investigated in the present paper is whether – and more specifically how and to what extent – such a translation can be automated for arbitrary temporal properties. More specifically, we focus solely on the *first* step, i.e. translation from temporal logic to rewrite

propositions. The second step is an entirely different problem, and is out of the scope of this paper.

Related work. In recent years, new results in rewriting logic have deeply extended the spectrum of its applications [9,17,5,16], especially in relation with temporal logic for rewriting [14,2]. Unlike [2], where LTL model checking is performed over finite structures, our approach handles temporal formulæ over infinite state systems. In this sense, it is close to [9]. However, in spite of its simplicity for practical applications, it does not permit – in its current state, at least – to consider equational theories. Our viewpoint differs slightly from other regular model-checking approaches such as Regular LTL [6] in that the temporal property relates to sequences of *actions* as opposed to sequences of *states*. It is however very similar to the method presented in [15], when reducing the equational theory to the identity.

Organisation of the paper. Section 2 presents the notions and notations in use throughout this paper, including the choice of temporal semantics and a precise statement of the problem at hand. Section 3[p6] deals with the main contributions of the paper: the translation rules and the technical tools (signatures, weak/strong intertwined semantics, etc) on which they depend.

2 Preliminaries & Problem Statement

The *extended naturals* are denoted by $\overline{\mathbb{N}} \triangleq \mathbb{N} \cup \{+\infty\}$ and $[\![n, m]\!]$ denotes the integer interval $[n, m] \cap \mathbb{Z}$, with the convention that $[\![0, +\infty]\!] = \mathbb{N}$. For any $k \in \mathbb{N}$, $\mathbb{N}_k \triangleq [\![k, +\infty]\!]$ and $\overline{\mathbb{N}}_k \triangleq \mathbb{N}_k \cup \{+\infty\}$. The powerset of S is written $\wp(S)$. Substitution is written $f[v/X]$, meaning "v replaces X in the expression f".

2.1 Rewrite Words & Maximal Rewrite Words

A comprehensive survey on term rewriting can be found in [8]. Let $\mathcal{T}(\mathbb{A})$ be the set of all terms on a ranked alphabet $\mathbb{A}$, let $\mathcal{R}$ be a finite rewrite system, and $\Pi \subseteq \mathcal{T}(\mathbb{A})$ any set of terms. A *finite or infinite word on* $\mathcal{R}$ is an element of

$$\mathcal{W} \triangleq \bigcup_{n \in \overline{\mathbb{N}}} \left([\![1, n]\!] \to \mathcal{R} \right) \ .$$

The length $\#w \in \overline{\mathbb{N}}$ of a word w is defined as $\mathrm{Card}\,(\mathrm{dom}\, w)$. Note that the empty function – of graph $\varnothing \times \mathcal{R} = \varnothing$ – is a word, which we call the *empty word*, denoted

by λ. Let $w \in \mathcal{W}$ be a word of domain $[\![1, n]\!]$, for $n \in \overline{\mathbb{N}}$, and let $m \in \mathbb{N}_1$; then the m-*suffix of* w is the word denoted by w^m, such that

$$w^m \triangleq \left| \begin{array}{ccc} [\![1, n-m+1]\!] & \longrightarrow & \mathcal{R} \\ k & \longmapsto & w(k+m-1) \end{array} \right. .$$

Note that $w^1 = w$, for any word w. The intuitive meaning that we attach to a word w is a sequence of rewrite rules of $\mathcal{R}$, called in succession – in other words, it represents a "run" of the TRS $\mathcal{R}$. Of course, there is nothing in the above definition of words that guarantees that such a sequence is in any way feasible, and such a notion only makes sense with respect to initial terms to be rewritten. Thus we now define the *maximal rewrite words of* $\mathcal{R}$*, originating in* Π:

$${}^{\mathcal{R}}(\!|\Pi|\!) \triangleq \left\{ w \in \mathcal{W} \;\middle|\; \begin{array}{l} \exists u_0 \in \Pi : \exists u_1, \ldots, u_{\#w} \in \mathcal{T}(\mathbb{A}) : \forall k \in \operatorname{dom} w, \\ u_{k-1} \xrightarrow{w(k)} u_k \;\wedge\; \#w \in \mathbb{N} \Rightarrow \mathcal{R}(\{u_{\#w}\}) = \varnothing \end{array} \right\} .$$

Note the potential presence of the empty word in that set. Informally, a word w is in ${}^{\mathcal{R}}(\!|\Pi|\!)$ if and only if the rewrite rules $w(1), \ldots, w(n), \ldots$ can be activated in succession, starting from a term $u_0 \in \Pi$, and the word w is "maximal" in the sense that it cannot be extended. That is to say, w ends only when no further rewrite rule can be activated. Thus ${}^{\mathcal{R}}(\!|\Pi|\!)$ captures the behaviours (or runs) of $\mathcal{R}$, starting from Π; this notion corresponds to the full paths of the rewrite graph described in [7].

2.2 Defining Temporal Semantics on Rewrite Words

Choice of LTL & Syntax. Before starting to think about translating temporal logic formulæ on rewrite words, we need to define precisely the kind of temporal formulæ under consideration, and their semantics. Given that prior work in [7] was done on LTL, and that our aim is to *generalise* this work, LTL – with subsets of $\mathcal{R}$ as atomic proposition – seems a reasonable choice. In practice we shall use a slight variant with generalised weak and strong next operators; the reasons for this choice will be discussed when the semantics are examined. A formula $\varphi \in \mathrm{LTL}$ is generated by the following grammar:

$$\begin{array}{rl} \varphi := X \mid \neg\varphi \mid \varphi \wedge \varphi \mid \bullet^m \varphi \mid \circ^m \varphi \mid \varphi \,\mathbf{U}\, \varphi & X \in \wp(\mathcal{R}) \\ \top \mid \bot \mid \varphi \vee \varphi \mid \varphi \Rightarrow \varphi \mid \Diamond\, \varphi \mid \Box\, \varphi & m \in \mathbb{N}\,. \end{array}$$

Note that the operators which appear on the first line are functionally complete; the remaining operators are defined syntactically as: $\top \triangleq \mathcal{R} \vee \neg\mathcal{R}$, $\bot \triangleq \neg\top$, $\varphi \vee \psi \triangleq \neg(\neg\varphi \wedge \neg\psi)$, $\varphi \Rightarrow \psi \triangleq \neg\varphi \vee \psi$, $\Diamond\, \varphi \triangleq \top \,\mathbf{U}\, \varphi$ and $\Box\, \varphi \triangleq \neg \Diamond \neg\varphi$.

Choice of Semantics. In the literature, the semantics of LTL are defined and well-understood for ω-words; however the words of ${}^{\mathcal{R}}(\!|\Pi|\!)$ may be infinite *or* finite, or even empty, which corresponds to the fact that, depending on its input, a rewrite system may either not terminate, terminate after some rewrite operations, or terminate immediately. Therefore we need semantics capable of accommodating both ω-words and finite words, as well as the edge-case of the empty word. In contrast to the classical case of ω-words, there are several ways to define (two-valued) semantics for LTL on finite, maximal words. One such way found in the literature is Finite-LTL (F-LTL) [13], which complements the long-standing use of a "strong" *next* operator introduced in [12] by coining a "weak" *next* variant. Figure 1 [p5] presents our choice of semantics for this paper,

$$
\begin{array}{lll}
(w,i) \models X & \text{iff} & i \in \operatorname{dom} w \text{ and } w(i) \in X \\
(w,i) \models \neg\varphi & \text{iff} & (w,i) \not\models \varphi \\
(w,i) \models (\varphi \wedge \psi) & \text{iff} & (w,i) \models \varphi \text{ and } (w,i) \models \psi \\
(w,i) \models \bullet^m \varphi & \text{iff} & i+m \in \operatorname{dom} w \text{ and } (w,i+m) \models \varphi \\
(w,i) \models \circ^m \varphi & \text{iff} & i+m \notin \operatorname{dom} w \text{ or } (w,i+m) \models \varphi \\
(w,i) \models \varphi \,\mathbf{U}\, \psi & \text{iff} & \exists j \in \operatorname{dom} w : j \geqslant i \wedge \begin{cases} (w,j) \models \psi & \wedge \\ \forall k \in [\![i, j-1]\!],\ (w,k) \models \varphi \end{cases}
\end{array}
$$

For any $w \in \mathcal{W}$, $i \in \mathbb{N}_1$, $m \in \mathbb{N}$ and $X \in \wp(\mathcal{R})$.

Fig. 1: LTL Semantics on Maximal Rewrite Words

which is essentially F-LTL with generalised next operators and the added twist that words *may* be infinite or empty. Note that $\bullet^1$ and $\circ^1$ correspond exactly to the classical strong and weak next operators, and that for $m \geqslant 1$, $\bullet^m$ (resp. $\circ^m$) can trivially be obtained by repeating $\bullet^1$ (resp. $\circ^1$) m times. So the only non-trivial difference here is the existence of $\bullet^0$ and $\circ^0$; this will prove quite convenient when we deal with the translation of $\Box$, using the following lemma.

Lemma 1 (*Weak-Next & Always*)**.** *Let* $\varphi \in$ LTL*,* $w \in \mathcal{W}$*,* $k \in \mathbb{N}$ *and* $i \in \mathbb{N}_1$*; it holds that* **(1)** $(w,i) \models \Box\varphi$ *iff* $(w,i) \models \bigwedge_{m=0}^{\infty} \circ^m \varphi$ *and* **(2)** $(w,i) \models \Box\varphi$ *iff* $(w,i) \models \bigwedge_{m=0}^{k-1} (\circ^m \varphi) \wedge \circ^k \Box\varphi$.

Before moving on, let us stress that the choice of semantics, or even the choice of LTL for that matter, should by no means be considered as etched in stone; it is very much a variable of the general problem. However it will henceforth be considered as data for the purposes of this paper.

TRS & LTL. Let φ be an LTL formula. We say that a word w satisfies/is a model of φ (denoted by $w \models \varphi$) iff $(w,1) \models \varphi$. Alternatively, we have $(w,i) \models \varphi$ iff

$w^i \models \varphi$. We say that the rewrite system $\mathcal{R}$, with initial language Π, satisfies/is a model of φ (denoted by $\mathcal{R}, \Pi \models \varphi$) iff $\forall w \in {}^{\mathcal{R}}(\!|\Pi|\!),\ w \models \varphi$.

2.3 Rewrite Propositions & Problem Statement

A *rewrite proposition on $\mathcal{R}$, from Π* is a formula of propositional logic whose atoms are language or rewrite systems comparisons. More specifically, a rewrite proposition π is generated by the following grammar:

$$\pi := \gamma \mid \gamma \wedge \gamma \mid \gamma \vee \gamma \qquad \gamma := \ell = \varnothing \mid X \subseteq X \mid \ell \subseteq \ell \qquad X \in \wp(\mathcal{R})\ .$$
$$\ell := \Pi \mid \mathcal{T}(\mathbb{A}) \mid X(\ell) \mid X^{-1}(\ell) \mid X^*(\ell)$$

Since the comparisons γ have obvious truth values, the interpretation of rewrite propositions is trivial; thus we will not introduce any notation for it, and automatically confuse π with its truth value in the remainder of this paper. Note that while other operators for propositional logic could be added, conjunction and disjunction will be enough for our purposes.

Problem Statement. We have now done enough groundwork to state our problem more formally. Given a rewrite system $\mathcal{R}$, a temporal formula φ in LTL (or some fragment of LTL), and an initial language $\Pi \subseteq \mathcal{T}(\mathbb{A})$, we search for an algorithmic method of building a rewrite proposition π such that $\mathcal{R}, \Pi \models \varphi$ if and only if π holds. We call such a method, as well as its result, an *exact translation* of φ, and say that π translates φ. If π is only a sufficient (resp. necessary) condition, then it is an *under-approximated* (resp. *over-approximated*) translation.

3 Building Translation Rules

3.1 Overview & Intuitions of the Translation

The Base Cases. Counterintuitively, $\varphi = \neg X$ is actually a simpler case than $\varphi = X$ as far as the translation is concerned, so we will consider it first. Case 1: Negative Literal. Suppose $\mathcal{R}, \Pi \models \neg X$. Recalling the semantics in Fig. 1[p5], this means that no term of Π can be rewritten by a rule in X. They *may* or *may not* be rewritable by rules *not* in X, though. Consider now $\pi_1 \equiv X(\Pi) = \varnothing$; it is easy to become convinced that this is an exact translation. Case 2: Positive Literal. Let $\varphi = X$. A first intuition would be that this is *roughly* the same case as before, but with the complement of X wrt. $\mathcal{R}$. So we write $\pi_2 \equiv [\mathcal{R} \setminus X](\Pi) = \varnothing$. This, however, is not strong enough. It translates the fact that *only* rules of X can rewrite Π.

But again, while X *may* in fact rewrite Π, there is nothing in π_2 to enforce that. Looking at the semantics, *all* possible words of ${}^{\mathcal{R}}(\!|\Pi|\!)$ *must* have at least one move (i.e. $1 \in \operatorname{dom} w$); this condition must be translated. It is equivalent to saying that all terms of Π are rewritable, which is expressed by $\Pi \subseteq \mathcal{R}^{-1}(\mathcal{T}(\mathbb{A}))$. More specifically, since we already impose that they are not rewritable by $\mathcal{R} \setminus X$, we can even write directly that they are rewritable by X, i.e. $\Pi \subseteq X^{-1}(\mathcal{T}(\mathbb{A}))$. Putting those two conditions together, we obtain $\pi_2' \equiv [\mathcal{R} \setminus X](\Pi) = \varnothing \wedge \Pi \subseteq X^{-1}(\mathcal{T}(\mathbb{A}))$, and this is an exact translation.

Of Strength & Weakness. Let us reflect on the previous cases for a minute; the immediate intuition is that X is *stronger* than $\neg X$, in the sense that whenever we see X, we must write an additional clause – enforcing rewritability – compared to $\neg X$. This actually depends on the context, as the next example will show. Case 3: Always Negative. Let $\varphi = \Box \neg X$. This means that neither the terms of Π nor their successors can be rewritten by X; in other words $\pi_3 \equiv X\left(\mathcal{R}^*(\Pi)\right) = \varnothing$. The translation is almost the same as for $\neg X$, the only difference being the use of $\mathcal{R}^*(\Pi)$ (Π and successors) instead of just Π as in π_1. More formally, $\pi_3 \equiv \pi_1[\mathcal{R}^*(\Pi)/\Pi]$. Case 4: Always Positive. Seeing this, one is tempted to infer that the same relationship that exists between the translations of $\neg X$ and $\Box \neg X$ exists as well between those of X and $\Box X$. In the case $\varphi = \Box X$, this would yield $\pi_4 \equiv \pi_2'[\mathcal{R}^*(\Pi)/\Pi] \equiv [\mathcal{R} \setminus X]\left(\mathcal{R}^*(\Pi)\right) = \varnothing \wedge \mathcal{R}^*(\Pi) \subseteq X^{-1}(\mathcal{T}(\mathbb{A}))$. But clearly this translation is much too strong as its second part implies that every term of Π can be rewritten by X, and so can all of the successors; consequently, ${}^{\mathcal{R}}(\!|\Pi|\!)$ must form an ω-language. Yet we have for instance $\lambda \models \Box X$ —note incidentally that $\lambda \models \Box \psi$ holds vacuously for any ψ. In general, under the semantics for $\Box$, words of any length, infinite, finite or nought, may satisfy $\Box X$. Thus the correct translation was simply $\pi_4' \equiv [\mathcal{R} \setminus X]\left(\mathcal{R}^*(\Pi)\right) = \varnothing$. So, unlike Cases 1 and 2, X is *not* in any sense stronger than $\neg X$ when behind a $\Box$. This is an important point which we shall need to keep track of during the translation; that necessary bookkeeping is the reason for the introduction of the weak and strong intertwined semantics described in Section 3.2[p9].

Conjunction, Disjunction & Negation. Case 5: And & Or. It is pretty clear that if π_5 translates φ and π_5' translates ψ, then $\pi_5 \wedge \pi_5'$ translates $\varphi \wedge \psi$. This holds thanks to the implicit universal quantifier, as we have $(\mathcal{R}, \Pi \models \varphi \wedge \psi) \iff (\mathcal{R}, \Pi \models \varphi) \wedge (\mathcal{R}, \Pi \models \psi)$. Contrariwise, the same does not hold for the disjunction,

and we have no general solution [(a)] to handle it. Given that one of the implications still holds, namely $(\mathcal{R}, \Pi \models \varphi \vee \psi) \iff (\mathcal{R}, \Pi \models \varphi) \vee (\mathcal{R}, \Pi \models \psi)$, a crude under-approximation can still be given if all else fails: $\pi_5 \vee \pi'_5 \implies \mathcal{R}, \Pi \models \varphi \vee \psi$.
Case 6: Negation. Although we have seen in Case 1 that a negative literal can easily be translated, negation cannot be handled in all generality by our method. Note that, because of the universal quantification, $\mathcal{R}, \Pi \not\models \varphi \neq \mathcal{R}, \Pi \models \neg\varphi$; thus the fact that π_6 translates φ does *not* a priori imply that $\neg\pi_6$ translates $\neg\varphi$. This is why we will assume in practice that input formulæ are provided in Negative Normal Form, which is licit as the presence of *both* weak and strong next operators enables any formula to be put in NNF.

Handling Material Implication. Case 7. We have just seen in Cases 5 and 6 that we can provide exact translations for neither negation nor disjunction. Inasmuch as $\varphi \Rightarrow \psi$ is defined as $\neg\varphi \vee \psi$, must material implication be forgone as well? An example involving an implication has been given in the introduction (page 1), so it would seem that a translation can be provided in at least *some* cases. Let us take the simple example $X \Rightarrow \bullet Y$. Assuming that any term $u \in \Pi$ is rewritten into some u' by a rule in X, then u' must be rewritable by Y, and only by Y. The set of X-successors of Π being $X(\Pi)$, those conditions yield the translation $\pi_7 \equiv X(\Pi) \subseteq Y^{-1}\left(\mathcal{T}(\mathbb{A})\right) \wedge [\mathcal{R} \setminus Y]\left(X(\Pi)\right) = \varnothing$. Note that the way in which implication has been handled here is very different from the approach taken for the other binary operators, which essentially consists in splitting the formula around the operator and translating the two subparts separately. In contrast, the antecedent of the implication was "assumed", whilst the consequent was translated as usual. In fact, recalling that π'_2 translates X, and thus $\pi''_2 \equiv \pi'_2[Y/X]$ translates Y, we have $\pi_7 \equiv \pi''_2[X(\Pi)/\Pi]$. So, "assuming" the antecedent consisted simply in changing our set of reachable terms —which we will from now on call the *past*, hence the notation Π. This is not an isolated observation; if π_0 denotes the translation of $\Box(X \Rightarrow \bullet Y)$ given in the introduction, then $\pi_0 \equiv \pi_7[\mathcal{R}^*(X(\Pi))/X(\Pi)]$. Thus "updating" the past is enough of a tool to deal with some simple uses of $\Box$ and implication... but consider the following formula: $\bullet Y \Rightarrow X$. In that case the antecedent lies in the future, relatively to the consequent. Therefore, in order to deal with all cases, we need some means of making assumptions about both past and future. This is the goal of the *signatures* presented in Section 3.3[p10].

[(a)] There are however special cases where disjunction can be translated exactly; see rules $(\vee^{\Rightarrow}_{\wedge})$[p15] and $(\vee^{\neg}_{\Rightarrow})$.

3.2 Weak and Strong Semantics for LTL

Restricting the Fragment. As mentioned in Cases 3 and 4 of the previous section, we will in practice be restricted to working with formulæ provided in Negative Normal Form. Furthermore, there are operators, such as $\Diamond$, for which we think that no translation *can* be provided, because rewrite propositions are not expressive enough —in particular, $\mathcal{R}^*(\Pi)$ hides all information regarding finite or infinite traces. If this is the case, then none of the operators of the "Until" family $\{\Diamond, \mathbf{U}, \mathbf{W}, \mathbf{R}, \ldots\}$ can be dealt with. Consequently, we are restricted to the following fragment of LTL, which will be denoted by $\mathcal{R}$-LTL:

$$\begin{aligned} \varphi := X \mid \neg X \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \Rightarrow \varphi \mid \quad & X \in \wp(\mathcal{R}) \\ \bullet^m \varphi \mid \circ^m \varphi \mid \Box \varphi \quad & m \in \mathbb{N}\,. \end{aligned}$$

Bookkeeping. (cf. Sec. 3.1[p6], case 4) In order to address the question of whether the translation of an atom X should be "strong" – enforce rewritability – or "weak", information is needed from the context. Namely, does the atom appear in the direct scope of a $\Box$? We solve this by introducing intertwined *weak semantics* – written $\models^{\mathbf{w}}$ – and *strong semantics* – written $\models^{\mathbf{s}}$, given in Fig. 2. For $\mu \in \{\mathbf{w}, \mathbf{s}\}$

$(w,i) \models^\mu \top$	$(w,i) \not\models^\mu \bot$	
$(w,i) \models^{\mathbf{s}} X$	iff	$i \in \operatorname{dom} w$ and $w(i) \in X$
$(w,i) \models^{\mathbf{w}} X$	iff	$i \notin \operatorname{dom} w$ or $w(i) \in X$
$(w,i) \models^\mu \neg X$	iff	$i \notin \operatorname{dom} w$ or $w(i) \notin X$
$(w,i) \models^\mu (\varphi \vee \psi)$	iff	$(w,i) \models^\mu \varphi$ or $(w,i) \models^\mu \psi$
$(w,i) \models^\mu (\varphi \wedge \psi)$	iff	$(w,i) \models^\mu \varphi$ and $(w,i) \models^\mu \psi$
$(w,i) \models^\mu (\varphi \Rightarrow \psi)$	iff	$(w,i) \models^{\mathbf{s}} \varphi \implies (w,i) \models^{\mathbf{s}} \psi$
$(w,i) \models^\mu \bullet^m \varphi$	iff	$i + m \in \operatorname{dom} w$ and $(w, i+m) \models^{\mathbf{s}} \varphi$
$(w,i) \models^\mu \circ^m \varphi$	iff	$i + m \notin \operatorname{dom} w$ or $(w, i+m) \models^{\mathbf{w}} \varphi$
$(w,i) \models^\mu \Box \varphi$	iff	$\forall j \in \operatorname{dom} w,\ j \geqslant i \Rightarrow (w,j) \models^{\mathbf{w}} \varphi$

For any $m \in \mathbb{N}$, $\mu \in \{\mathbf{w}, \mathbf{s}\}$

Fig. 2: $\mathcal{R}$-LTL Weak & Strong Semantics

the notations $w \models^\mu \varphi$ and $\mathcal{R}, \Pi \models^\mu \varphi$ are defined in the same way as for $\models$. How those semantics are used will become clearer in section 3.4[p15], where the translation rules are given. The important point for now is that the strong semantics are equivalent to the normal semantics of LTL on the fragment $\mathcal{R}$-LTL, which is shown by Lemma 3.

Lemma 2 (*Strong-Weak Domain-Equivalence*)**.** *For all w, φ, i, it holds that* $i \in \operatorname{dom} w \implies (w,i) \models^{\mathbf{s}} \varphi \Leftrightarrow (w,i) \models^{\mathbf{w}} \varphi$.

Lemma 3 (*Strong Semantics*)**.** *For all words* $w \in \mathcal{W}$ *and all formulæ* $\varphi \in \mathcal{R}$-LTL*, we have* $\forall i \in \mathbb{N}_1,\ (w,i) \models^{s} \varphi \iff (w,i) \models \varphi$.

3.3 Girdling the Future: Signatures

As discussed in Sec. 3.1[p6], Case 7, implication is handled by converting the antecedent φ of a formula $\varphi \Rightarrow \psi$ into "assumptions". Concretely, this consists in building a model of φ – called a *signature* of φ, written $\xi(\varphi)$ – which can be manipulated during the translation. The variety of signatures defined hereafter handles formulæ φ within the fragment $\mathcal{A}$-LTL ($\mathcal{A}$ for **a**ntecedent), which is $\mathcal{R}$-LTL without $\vee$ or $\Rightarrow$. This section covers the technical tools needed for building signatures (Fig. 3[p13]) and understanding the translation rules (Sec. 3.4[p15]).

Definitions. Signatures. A *signature* σ is an element of the space

$$\Sigma = \bigcup_{n\in\mathbb{N}} \Big[\big([\![1,n]\!] \cup \{\omega\} \big) \to \wp(\mathcal{R}) \Big] \times \wp(\overline{\mathbb{N}}) \ .$$

Core, Support, Domain, Cardinal. Let $\sigma = (f,S)$; then the function f is called the *core of* σ, denoted by $\partial\sigma$, and S is called its *support*, written $\nabla\sigma$. The *domain of* σ is defined as $\operatorname{dom}\sigma \triangleq \operatorname{dom} f \setminus \{\omega\}$, and its *cardinal* is $\#\sigma \triangleq \operatorname{Card}(\operatorname{dom}\sigma)$. Special Notations, Empty Signature. A signature $\sigma = (f,S)$ will be written either compactly as $\sigma = \wr f \mid S \int$, or *in extenso* as $\wr f(1), f(2), \ldots, f(\#\sigma) \fatsemi f(\omega) \mid S \int$. We denote by $\varepsilon \triangleq \wr \fatsemi \mathcal{R} \mid \overline{\mathbb{N}} \int$ the *empty signature*. Let $k \in \mathbb{N}_1 \cup \{\omega\}$, then we write

$$\sigma[k] \triangleq \begin{cases} f(k) & \text{if } k \in \operatorname{dom}\sigma \\ f(\omega) & \text{if } k \notin \operatorname{dom}\sigma \end{cases} .$$

Signature Product. Let σ and σ' two signatures; then their *product* is another signature defined as $\sigma \otimes \sigma' \triangleq \wr g \mid \nabla\sigma \cap \nabla\sigma' \int$, where

$$g \triangleq \left| \begin{array}{ccc} \operatorname{dom}\partial\sigma \cup \operatorname{dom}\partial\sigma' & \longrightarrow & \wp(\mathcal{R}) \\ k & \longmapsto & \sigma[k] \cap \sigma'[k] \end{array} \right. .$$

Note that as a consequence, $\forall k \in \mathbb{N}_1,\ (\sigma\otimes\sigma')[k] = \sigma[k] \cap \sigma'[k]$. **(e.g.** Let $\sigma = \wr X, Y \fatsemi Z \mid \mathbb{N}_2 \int$ and $\rho = \wr X' \fatsemi Z' \mid \mathbb{N}_3 \int$; then $\sigma \otimes \rho = \wr X \cap X', Y \cap Z' \fatsemi Z \cap Z' \mid \mathbb{N}_3 \int$.**)**

Remark 4 (Summation Notation)**.** The set of signatures Σ, equipped with the signature-product $\otimes$, forms a commutative monoid whose neutral element is ε.

Convergence. Let $\rho = (\sigma_n)_{n\in\mathbb{N}}$ be an infinite sequence of signatures. It is *convergent* if **(1)** the sequence $(\nabla\sigma_n)_{n\in\mathbb{N}}$ converges towards a limit $\nabla\sigma_\infty$, and **(2)**

for all $k \in \mathbb{N}_1$, the sequence $(\sigma_n[k])_{n\in\mathbb{N}}$ converges towards a limit $\sigma_\infty[k]$, and **(3)** the sequence of limits $(\sigma_\infty[k])_{k\in\mathbb{N}_1}$ itself converges towards a limit $\sigma_\infty[\infty]$. We call this sequence the *limit core*. It is not directly in the form of a bona fide signature core. However, its co-domain being $\wp(\mathcal{R})$, which is finite, there exists a rank $N \geqslant 0$ such that for all $k > N$, $\sigma_\infty[k] = \sigma_\infty[\infty]$, and thus, taking the smallest such N, we define $\wr \sigma_\infty[1], \ldots, \sigma_\infty[N] \fatsemi \sigma_\infty[\infty] \mid \nabla\sigma_\infty \int$ to be the *limit* of ρ, which we denote by $\lim \rho$ or $\lim_{n\to\infty} \sigma_n$, or more simply by σ_∞. Note that the core of the limit is equivalent to the limit core, in the intuitive sense that they define the same constrained words. Otherwise ρ is *divergent*, and its limit is left undefined. **(e.g.** The sequence $(\wr \mathcal{R}_1, \ldots \mathcal{R}_n, X \fatsemi \mathcal{R} \mid [\![1, n]\!] \int)_{n\in\mathbb{N}}$, with $\mathcal{R}_i = \mathcal{R}\ \forall i$, converges towards $\wr \fatsemi X \mid \mathbb{N} \int$. **)** Infinite Products. Remark 4 legitimates the use of a Sigma-notation $\bigotimes_{k=l}^{m} \sigma_k$ for $\sigma_l \otimes \sigma_{l+1} \otimes \cdots \otimes \sigma_m$, with the usual properties. We define a notion of *infinite product* of signatures as well, in the classical way: the infinite product $\bigotimes_{k=l}^{\infty} \sigma_k$ converges if and only if the associated sequence of partial products $(\bigotimes_{k=l}^{n} \sigma_k)_{n\in\mathbb{N}_l}$ converges, and in that case

$$\bigotimes_{k=l}^{\infty} \sigma_k \triangleq \lim_{n\to\infty} \bigotimes_{k=l}^{n} \sigma_k \ .$$

Constrained Words. The *words of* $\mathcal{R}$*, originating in* Π *and constrained by* σ are defined by ${}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \triangleq \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma \wedge \forall k \in \operatorname{dom} w,\ w(k) \in \sigma[k] \right\}$. **(e.g.** Let $\sigma = \wr X, Y \fatsemi Z \mid \mathbb{N}_2 \int$; then its core is the function $\partial\sigma = \{ 1 \mapsto X, 2 \mapsto Y, \omega \mapsto Z \}$, its domain is $\operatorname{dom}\sigma = [\![1, 2]\!]$, its support is $\nabla\sigma = \mathbb{N}_2$, its cardinal is $\#\sigma = 2$, and we have $\sigma[1] = X$, $\sigma[2] = Y$, $\sigma[3] = \sigma[4] = \cdots = \sigma[\omega] = Z$. Its constrained words are the maximal words of length at least 2, whose first two letters are in X and Y, respectively, and whose other letters are all in Z.**)** Lemma 5 serves in the base cases of signature-building, and Lem. 6 in the constructions of $\xi(\varphi \wedge \psi)$ and $\xi(\Box\,\varphi)$, and rule $(\Rightarrow_\Sigma)_{[p15]}$;

Lemma 5 (*No Constraints*)**.** *We have* ${}^{\mathcal{R}}(\!|\Pi \fatsemi \varepsilon|\!) = {}^{\mathcal{R}}(\!|\Pi|\!)$.

Lemma 6 (*Breaking Products*)**.** *For any signatures* $\sigma, \sigma' \in \Sigma$*, and any language* Π*, we have* **(1)** ${}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma \otimes \sigma'|\!) = {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \cap {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma'|\!)$*. Furthermore, this generalises to infinitary cases:* **(2)** *given a sequence* $(\sigma_n)_{n\in\mathbb{N}}$ *such that the infinite product* $\bigotimes_{n=0}^{\infty} \sigma_n$ *converges, it holds that* ${}^{\mathcal{R}}(\!|\Pi \fatsemi \bigotimes_{n=0}^{\infty} \sigma_n|\!) = \bigcap_{n=0}^{\infty} {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma_n|\!)$.

Arithmetic Overloading. We overload the operators $+$ and $-$ on the profile $\wp(\overline{\mathbb{N}}) \times \mathbb{N} \to \wp(\overline{\mathbb{N}})$ such that, for any $S \in \wp(\overline{\mathbb{N}})$ and $n \in \mathbb{N}$, we have $S + n \triangleq \{ k + n \mid k \in S \}$ and $S - n \triangleq \{ k - n \mid k \in S \} \cap \overline{\mathbb{N}}$. Shifts Left & Right. Let $m \in \mathbb{N}$;

then we define the *strong* m*-left shift of* σ as $\sigma \blacktriangleleft m \triangleq \wr \partial\sigma(m+1), \ldots, \partial\sigma(\#\sigma) \fatsemi \partial\sigma(\omega) \mid (\nabla\sigma - m) \setminus \{0\} \wr$ and the *weak* m*-left shift of* σ as $\sigma \triangleleft m \triangleq \wr \partial\sigma(m+1), \ldots, \partial\sigma(\#\sigma) \fatsemi \partial\sigma(\omega) \mid \nabla\sigma - m \wr$. Conversely, the *strong* m*-right shift of* σ is $\sigma \blacktriangleright m \triangleq \wr \mathcal{R}_1, \ldots, \mathcal{R}_m, \partial\sigma(1), \ldots, \partial\sigma(\#\sigma) \fatsemi \partial\sigma(\omega) \mid (\nabla\sigma \setminus \{0\}) + m \wr$, while the *weak* m*-right shift of* σ is $\sigma \triangleright m \triangleq \wr \mathcal{R}_1, \ldots, \mathcal{R}_m, \partial\sigma(1), \ldots, \partial\sigma(\#\sigma) \fatsemi \partial\sigma(\omega) \mid [\![0, m]\!] \cup (\nabla\sigma + m) \wr$, with $\mathcal{R}_1 = \mathcal{R}, \ldots, \mathcal{R}_m = \mathcal{R}$. Note that for all $m \in \mathbb{N}$ and all $k \in \mathbb{N}_1$, $(\sigma \triangleleft m)[k] = \sigma[k+m]$, for all $k \leqslant m$, $(\sigma \blacktriangleright m)[k] = (\sigma \triangleright m)[k] = \mathcal{R}$ and for all $k > m$, $(\sigma \blacktriangleright m)[k] = (\sigma \triangleright m)[k] = \sigma[k-m]$. **(e.g.** Let $\sigma = \wr X, Y \fatsemi Z \mid \mathbb{N}_2 \wr$; then $\sigma \blacktriangleleft 1 = \sigma \triangleleft 1 = \wr Y \fatsemi Z \mid \mathbb{N}_1 \wr$, $\sigma \blacktriangleright 1 = \wr \mathcal{R}, X, Y \fatsemi Z \mid \mathbb{N}_3 \wr$, and $\sigma \triangleright 1 = \wr \mathcal{R}, X, Y \fatsemi Z \mid \mathbb{N} \setminus \{2\} \wr$. **)**

Lemma 7 justifies the fact that the computation of $\xi(\Box\, \varphi)$ always yields a useable signature; a closed form of the limit is given in the proof.

Lemma 7 (*Automatic Convergences*)**.** *Let* $(\sigma_n)_{n\in\mathbb{N}}$ *be any sequence of signatures, and* $(\rho_n)_{n\in\mathbb{N}}$ *its associated sequence of partial products* $(\bigotimes_{i=0}^{n} \sigma_i)_{n\in\mathbb{N}}$*. Then* $(\rho_n)_{n\in\mathbb{N}}$ *satisfies convergence criteria* (1) *and* (2)*. Furthermore, if* σ *is a given signature and* $\sigma_i = \sigma \blacktriangleright i$ *or* $\sigma_i = \sigma \triangleright i$*, for any* $i \in \mathbb{N}$*, then criterion* (3) *is satisfied as well, and the infinite product* $\bigotimes_{n=0}^{\infty} \sigma_n$ *converges.*

Proof. **(1)** For all $n \in \mathbb{N}$, $\nabla\rho_n = \bigcap_{i=0}^{n} \nabla\sigma_i$, thus it is clear that $\nabla\rho_n = \bigcap_{i=0}^{n} \nabla\sigma_i \supseteq \bigcap_{i=0}^{n+1} \nabla\sigma_i = \nabla\rho_{n+1}$ or, in other words, $(\nabla\rho_n)_{n\in\mathbb{N}}$ is a (trivial) contracting sequence of finite sets. Therefore it converges towards $\bigcap_{i=0}^{\infty} \nabla\sigma_i$. **(2)** Let $k \in \mathbb{N}_1$; we have

$$\rho_n[k] = \left(\bigotimes_{i=0}^{n} \sigma_i\right)[k] = \bigcap_{i=0}^{n} \sigma_i[k] \ ,$$

and thus $\rho_n[k] = \bigcap_{i=0}^{n} \sigma_i[k] \supseteq \bigcap_{i=0}^{n+1} \sigma_i[k] = \rho_{n+1}[k]$ and again, $(\rho_n[k])_{n\in\mathbb{N}}$ is a trivial contracting sequence of finite sets; therefore it converges towards a limit which we denote by $\rho_\infty[k] = \bigcap_{i=0}^{\infty} \sigma_i[k]$. **(3)** Suppose now that $\sigma_i = \sigma \triangleright i$ (resp. $\sigma_i = \sigma \blacktriangleright i$, the computation will be unchanged), we have

$$\begin{aligned}\rho_\infty[k] = \bigcap_{i=0}^{\infty} \sigma_i[k] = \bigcap_{i=0}^{\infty} (\sigma \triangleright i)[k] &= \left(\bigcap_{i=0}^{k-1} (\sigma \triangleright i)[k]\right) \cap \left(\bigcap_{i=k}^{\infty} (\sigma \triangleright i)[k]\right) \\ &= \left(\bigcap_{i=0}^{k-1} \sigma[k-i]\right) \cap \left(\bigcap_{i=k}^{\infty} \mathcal{R}\right) = \bigcap_{i=0}^{k-1} \sigma[k-i] = \bigcap_{i=1}^{k} \sigma[i] \ .\end{aligned}$$

Given that for all $i > \#\sigma$, $\sigma[i] = \sigma[\omega]$, it follows that for all $k > \#\sigma$, $\rho_\infty[k] = \bigcap_{i=1}^{\#\sigma+1} \sigma[i]$. Thus $(\rho_\infty[k])_{k\in\mathbb{N}_1}$ converges. This shows that the infinite product $\bigotimes_{n=0}^{\infty} \sigma_n$ is convergent. □

Building Signatures. Figure 3[p13] defines the function $\xi(\cdot) : \mathcal{A}\text{-LTL} \to \Sigma$. As Theorem 8 shows, the signature $\xi(\varphi)$ essentially captures a model of φ.

$$\xi(\top) \triangleq \wr \S \mathcal{R} \mid \overline{\mathbb{N}} \int = \varepsilon \qquad \xi(\bot) \triangleq \wr \S \varnothing \mid \varnothing \int$$
$$\xi(X) \triangleq \wr X \S \mathcal{R} \mid \overline{\mathbb{N}}_1 \int \qquad \xi(\neg X) \triangleq \wr \mathcal{R} \setminus X \S \mathcal{R} \mid \overline{\mathbb{N}} \int$$
$$\xi(\bullet^m \varphi) \triangleq \xi(\varphi) \blacktriangleright m \qquad \xi(\circ^m \varphi) \triangleq \xi(\varphi) \triangleright m$$
$$\xi(\varphi \wedge \psi) \triangleq \xi(\varphi) \otimes \xi(\psi) \qquad \xi(\Box \varphi) \triangleq \bigotimes_{m=0}^{\infty} \left[\xi(\varphi) \triangleright m \right]$$

Fig. 3: Building Signatures on $\mathcal{A}$-LTL

Theorem 8 (*Signatures*)**.** *For any* $\Pi \subseteq \mathcal{T}(\mathbb{A})$ *and any* $\varphi \in \mathcal{A}\text{-LTL}$*,*

$$^{\mathcal{R}}(\!|\Pi \S \xi(\varphi)|\!) = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \varphi \right\} .$$

3.4 The Translation Rules

Now that the main technical tools are in place, there remains to define what is meant by "translation rule", and to state the rules themselves. For any $\mu \in \{\mathbf{w}, \mathbf{s}\}$, $\varphi \in \text{LTL}$, $\Pi \subseteq \mathcal{T}(\mathbb{A})$, $\sigma \in \Sigma$, we define $\langle \Pi \S \sigma \Vdash^{\mu} \varphi \rangle$ as shorthand for $\forall w \in {}^{\mathcal{R}}(\!|\Pi \S \sigma|\!),\ w \models^{\mu} \varphi$. We call such a notation $\langle \Pi \S \sigma \Vdash^{\mu} \varphi \rangle$ a *translation block*. A *translation rule* is of the form

$$\updownarrow \frac{A \qquad P(\sigma, \varphi)}{E} \quad \text{or} \quad \uparrow \frac{A \qquad P(\sigma, \varphi)}{E} \quad \text{or} \quad ? \frac{A \qquad \uparrow P(\sigma, \varphi) \ \updownarrow Q(\sigma, \varphi)}{E} ,$$

where A stands for some translation block $\langle \Pi \S \sigma \Vdash^{\mu} \varphi \rangle$, $P, Q \in \Sigma \times \mathcal{R}\text{-LTL} \to \mathbb{B}$ are predicates on signatures and formulæ, and E is a mixed translation/reachability proposition. More precisely, E is generated by the grammar given in Sec. 2.3[p6], with the added production $\gamma := \Upsilon$, where Υ is a translation block. The $\updownarrow$-rules (exact translations) are defined to hold iff $P(\sigma, \varphi) \implies (A \Leftrightarrow E)$, the $\uparrow$-rules (under-approximations) hold iff $P(\sigma, \varphi) \implies (E \Rightarrow A)$, and the ?-rules hold iff $P(\sigma, \varphi) \implies (E \Rightarrow A)$ and $(P(\sigma, \varphi) \wedge Q(\sigma, \varphi)) \implies (A \Leftrightarrow E)$. When omitted, P is assumed to be $\top$.

Theorem 9 entails that any derivation (i.e. tree of rule applications with no translation blocks left in the leaves) starting with $\langle \Pi \S \varepsilon \Vdash^{\mathbf{s}} \varphi \rangle$ yields an exact translation of φ (if only exact rules are involved), or an under-approximation (if some $\uparrow$-rules are used).

Theorem 9 (*Translation Satisfaction*)**.** $\langle \Pi \fatsemi \varepsilon \Vdash^{s} \varphi \rangle \iff \mathcal{R}, \Pi \models \varphi$.

A few additional definitions and results about signatures are needed in order to justify some translation rules: Remark 10 is needed by rule $(\Box_{\hbar})_{[p15]}$; Lem. 13 intervenes in rules $(\bullet^{m})_{[p15]}$ and $(\circ^{m})$; Lem. 11 and Cor. 12 in rule $(\bullet^{m})$; Rmk. 14 and Lem. 15 in rule $(\Box_{*})$; Prp. $16_{[p15]}$ justifies that rule $(\Box_{\hbar})$ eventually terminates. Signature Iteration. Let $\Pi \subseteq \mathcal{T}(\mathbb{A})$ a language, and $\sigma \in \Sigma$ a signature; then for $n \in \mathbb{N}$ we let $\Pi^{n}_{\sigma} \triangleq \sigma[n]\left(\sigma[n-1]\left(\cdots \sigma[1]\left(\Pi\right)\cdots\right)\right)$ be the n-*iteration* of the signature σ. More formally, it is defined recursively such that $\Pi^{0}_{\sigma} \triangleq \Pi$ and $\Pi^{n+1}_{\sigma} \triangleq \sigma[n+1]\left(\Pi^{n}_{\sigma}\right)$. Length Rejector. For $n \in \mathbb{N}$, the rewrite proposition $\Psi^{\sigma}_{\Pi}(n)$ is called the n-*length rejector*, and defined as $\Psi^{\sigma}_{\Pi}(n) \triangleq \Pi^{n}_{\sigma} \subseteq \sigma[n+1]^{-1}\left(\mathcal{T}(\mathbb{A})\right)$. Strengthening. If σ is a signature, then $\star\sigma \triangleq \lbag \partial\sigma \mid \nabla\sigma \setminus \{0\} \rbag$ is its *strengthening*. Note that $(\sigma \blacktriangleleft m) = \star(\sigma \lhd m)$, for all m.

Remark 10 (Strengthening of Always)**.** Let $\Pi \subseteq \mathcal{T}(\mathbb{A})$, $\sigma \in \Sigma$, and $\varphi \in \mathcal{R}$-LTL. Then $\langle \Pi \fatsemi \sigma \Vdash^{\mu} \Box\varphi \rangle \iff \langle \Pi \fatsemi \star\sigma \Vdash^{\mu} \Box\varphi \rangle$.

Lemma 11. *Let σ be a signature and $\Pi \subseteq \mathcal{T}(\mathbb{A})$ a language; then for any $n \in \mathbb{N}$, the proposition $\Psi^{\sigma}_{\Pi}(n)$ holds iff for all $w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!)$, $\#w \neq n$.*

Corollary 12 (*Length Rejection*)**.** *Let $S \in \wp(\mathbb{N})$, σ a signature and Π a language; the rewrite proposition $\bigwedge_{n \in S \cap \nabla\sigma} \Psi^{\sigma}_{\Pi}(n)$ holds iff for all $w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!)$, $\#w \notin S$.*

Lemma 13 (*Shifting Words*)**.** *Let σ be a signature and $\Pi \subseteq \mathcal{T}(\mathbb{A})$ a language; then* ${}^{\mathcal{R}}(\!|\Pi^{m}_{\sigma} \fatsemi \sigma \lhd m|\!) = \left\{ w^{m+1} \;\middle|\; w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \wedge \#w \geqslant m \right\}$.

Remark 14 (Constrained Union)**.** Let $\sigma \in \Sigma$, $I \subseteq \mathbb{N}$, and for each $i \in I$, $\Pi_{i} \subseteq \mathcal{T}(\mathbb{A})$. Then $\bigcup_{i \in I} {}^{\mathcal{R}}(\!|\Pi_{i} \fatsemi \sigma|\!) = {}^{\mathcal{R}}(\!|\bigcup_{i \in I} \Pi_{i} \fatsemi \sigma|\!)$.

Stability. A signature $\sigma \in \Sigma$ is called *stable* if $\sigma \lhd 1 = \sigma$; this is equivalent to the condition $\#\sigma = 0$ and $\nabla\sigma \in \{\varnothing, \{+\infty\}, \mathbb{N}, \overline{\mathbb{N}}\}$, and also to the condition $\forall n \in \mathbb{N},\ \sigma \lhd n = \sigma$. High Point. The *high point* $\hbar\sigma$ of a signature σ is the smallest $h \in \mathbb{N}$ such that $\sigma \lhd h$ is stable. Note that σ is stable if and only if $\hbar\sigma = 0$. Given the characterisation of stability given above, an alternative definition of $\hbar\sigma$ would be the smallest $h \geqslant \#\sigma$ such that either $\mathbb{N}_{h} \subseteq \nabla\sigma$ or $\nabla\sigma \cap \mathbb{N}_{h} = \varnothing$. If no such h exists[(b)], we take by convention $\hbar\sigma = +\infty$. Low Point. The *low point* $\ell\sigma$ of a signature σ is the smallest length authorised by σ; more precisely, it is defined as $\ell\sigma \triangleq \min \nabla\sigma$.

[(b)] Consider a signature σ such that $\nabla\sigma$ is the set of odd numbers, or the set of prime numbers, for instance. Such a signature cannot be stabilised. Fortunately, Proposition $16_{[p15]}$ shows that such exotic cases are irrelevant to this paper.

Lemma 15 (*All Suffixes*)**.** *Let σ be a stable signature, and $\Pi \subseteq \mathcal{T}(\mathbb{A})$ a language. Then we have* $\left\{ w^{1+n} \;\middle|\; n \in \mathbb{N},\ w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \#w \geqslant n \right\} = {}^{\mathcal{R}}(\!|\sigma[\omega]^*(\Pi) \fatsemi \sigma|\!)$.

Proposition 16 (*Stability of $\xi(\cdot)$*)**.** *The signature of any formula $\varphi \in \mathcal{A}$-LTL is stabilisable; in other words, $\hbar\xi(\varphi) \in \mathbb{N},\ \forall \varphi \in \mathcal{A}$-LTL.*

Theorem 17 (*Translation*)**.** *All the following translation rules hold.*

$$\updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \top \rangle}{\top} \qquad (\top) \qquad\qquad \updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \bot \rangle}{\bot} \qquad (\bot)$$

$$\updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ X \wedge Y \rangle}{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ X \cap Y \rangle} \qquad (\wedge_X) \qquad\qquad \updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ X \vee Y \rangle}{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ X \cup Y \rangle} \qquad (\vee_X)$$

$$\updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \varphi \wedge \psi \rangle}{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \varphi \rangle \wedge \langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \psi \rangle} \qquad (\wedge)$$

$$\updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ [\varphi \vee \varphi'] \Rightarrow \psi \rangle}{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \varphi \Rightarrow \psi \rangle \wedge \langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \varphi' \Rightarrow \psi \rangle} \qquad (\vee^{\Rightarrow}_{\wedge})$$

$$\updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \varphi \vee \psi \rangle \qquad \neg\varphi \in \mathcal{A}\text{-LTL}}{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \neg\varphi \Rightarrow \psi \rangle} \qquad (\vee^{\neg}_{\Rightarrow})$$

$$\uparrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \varphi \vee \psi \rangle}{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \varphi \rangle \vee \langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \psi \rangle} \qquad (\vee_{\uparrow})$$

$$\updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \varphi \Rightarrow \psi \rangle}{\langle \Pi \fatsemi \sigma \otimes \xi(\varphi) \ \Vdash^{\mathbf{s}} \ \psi \rangle} \qquad (\Rightarrow_{\Sigma})$$

$$\updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \circ^m \varphi \rangle}{\langle \Pi^m_\sigma \fatsemi \sigma \blacktriangleleft m \ \Vdash^{\mathbf{w}} \ \varphi \rangle} \qquad (\circ^m)$$

$$\updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \bullet^m \varphi \rangle}{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \circ^m \varphi \rangle \wedge \bigwedge\limits_{n \in [\![0,m]\!] \cap \nabla\sigma} \Psi^{\sigma}_{\Pi}(n)} \qquad (\bullet^m)$$

$$\updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \Box \varphi \rangle \qquad \sigma \textit{ is stable}}{\langle \sigma[\omega]^*(\Pi) \fatsemi \star\sigma \ \Vdash^{\mathbf{w}} \ \varphi \rangle} \qquad (\Box_*)$$

$$\updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \Box \varphi \rangle \qquad \hbar\sigma \in \mathbb{N}_1}{\left\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \bigwedge\limits_{k=0}^{\hbar\sigma-1} \circ^k \varphi \right\rangle \wedge \left\langle \Pi^{\hbar\sigma}_{\sigma} \fatsemi \sigma \lhd \hbar\sigma \ \Vdash^{\mu} \ \Box \varphi \right\rangle} \qquad (\Box_{\hbar})$$

$$\updownarrow \frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \neg X \rangle}{\langle \Pi \fatsemi \sigma \ \Vdash^{\mathbf{w}} \ \mathcal{R} \setminus X \rangle} \qquad (\neg X)$$

Additionally, the following four rules are being explored as a possible coverage of the difficult case of the atom X. While the main bodies of those rules encompass all

the necessary translations, adjusting their exact respective application predicates is still ongoing work, which sets them apart from the proven formulæ of Thm. 17.

$$?\frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mathbf{w}} \ X\rangle \qquad \uparrow \ell\sigma \leqslant 1 \ \updownarrow \sigma \lhd 1 = \varepsilon}{\left[\mathcal{R} \setminus (X \cap \sigma[1])\right](\Pi) = \varnothing} \tag{$X^{\mathbf{w}}_{\ell\leqslant 1}$}$$

$$?\frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mathbf{s}} \ X\rangle \qquad \uparrow \ell\sigma = 0 \ \updownarrow \sigma \lhd 1 = \varepsilon}{\langle \Pi \fatsemi \sigma \ \Vdash^{\mathbf{w}} \ X\rangle \wedge \Pi \subseteq \left(X \cap \sigma[1]\right)^{-1}(\mathcal{T}(\mathbb{A}))} \tag{$X^{\mathbf{s}}_{\ell 0}$}$$

$$?\frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mathbf{s}} \ X\rangle \qquad \uparrow \ell\sigma = 1 \ \updownarrow \sigma \lhd 1 = \varepsilon}{\langle \Pi \fatsemi \sigma \ \Vdash^{\mathbf{w}} \ X\rangle} \tag{$X^{\mathbf{s}}_{\ell 1}$}$$

$$?\frac{\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ X\rangle \qquad \uparrow \ell\sigma \geqslant 2 \ \updownarrow \sigma \lhd \ell\sigma = \varepsilon}{\sigma[\ell\sigma]\left(\cdots \sigma[2]\left(\left[\mathcal{R} \setminus (X \cap \sigma[1])\right](\Pi)\right)\cdots\right) = \varnothing} \tag{$X^{\mu}_{\ell 2}$}$$

The general derivation algorithm consists in systematically applying the first rule that matches, starting with the block $\langle \Pi \fatsemi \varepsilon \ \Vdash^{\mathbf{s}} \ \varphi\rangle$. Let it be noted that not all of the given rules are strictly necessary. For instance ($\vee^{\Rightarrow}_{\wedge}$) corresponds to a basic tautology of propositional logic, which rewrites the formula in a form more amenable to translation. Similarly, rule ($\vee^{\neg}_{\Rightarrow}$) relies on a transformation of the antecedent into $\mathcal{A}$-LTL (which is not always possible, in which case the rule does not apply). While their presence is not fundamental to the system, they extend the number of translatable cases. There are doubtless many other such simplifications not listed here – an obvious one being the commutation of ($\vee^{\neg}_{\Rightarrow}$). This sensitivity of the translation to transformations of the input formula makes it difficult to give an exact characterisation of the supported fragment – it is not simply $\mathcal{R}$-LTL, restricted to $\mathcal{A}$-LTL for antecedents. For instance, even though $\Diamond$ cannot be translated in general, its presence in the NNF of the input φ is not enough in itself to assert that φ cannot be translated: if it appears in, say, $\Diamond X \vee \psi$, it can be handled using rule ($\vee^{\neg}_{\Rightarrow}$). We intend to expand the translatable fragment in future works; this will hopefully make it easier to characterise.

Example. Let us derive the translation of $\varphi = \Box(X \Rightarrow \bullet^1 Y)$.

$$\updownarrow \frac{\left\langle \Pi \fatsemi \varepsilon \ \Vdash^{\mathbf{s}} \ \Box(X \Rightarrow \bullet^1 Y)\right\rangle}{\updownarrow \dfrac{\left\langle \mathcal{R}^*(\Pi) \fatsemi \star\varepsilon \ \Vdash^{\mathbf{w}} \ X \Rightarrow \bullet^1 Y\right\rangle}{\updownarrow \dfrac{\left\langle \mathcal{R}^*(\Pi) \fatsemi \wr X \fatsemi \mathcal{R} \mid \overline{\mathbb{N}}_1 \int \ \Vdash^{\mathbf{s}} \ \bullet^1 Y\right\rangle}{\Psi^{\wr X \fatsemi \mathcal{R} \mid \overline{\mathbb{N}}_1 \int}_{\mathcal{R}^*(\Pi)}(1) \wedge \updownarrow \dfrac{\left\langle \mathcal{R}^*(\Pi) \fatsemi \wr X \fatsemi \mathcal{R} \mid \overline{\mathbb{N}}_1 \int \ \Vdash^{\mathbf{s}} \ \circ^1 Y\right\rangle}{\updownarrow \dfrac{\langle X(\mathcal{R}^*(\Pi)) \fatsemi \wr \fatsemi \mathcal{R} \mid \overline{\mathbb{N}}_1 \int \ \Vdash^{\mathbf{w}} \ Y\rangle}{[\mathcal{R} \setminus Y]\,(X(\mathcal{R}^*(\Pi))) = \varnothing}\,(X^{\mathbf{w}}_{\ell\leqslant 1})}\,(\circ^m)}\,(\bullet^m)}\,(\Rightarrow_\Sigma)}\,(\Box_*)} .$$

This yields the exact translation $[\mathcal{R} \setminus Y](X(\mathcal{R}^*(\Pi))) = \varnothing \wedge \Psi^{\wr X;\mathcal{R}|\overline{\mathbb{N}}_1 \int}_{\mathcal{R}^*(\Pi)}(1)$ which, once expanded, yields $[\mathcal{R} \setminus Y](X(\mathcal{R}^*(\Pi))) = \varnothing \wedge X(\mathcal{R}^*(\Pi)) \subseteq \mathcal{R}^{-1}(\mathcal{T}(\mathbb{A}))$. This is equivalent to $[\mathcal{R} \setminus Y](X(\mathcal{R}^*(\Pi))) = \varnothing \wedge X(\mathcal{R}^*(\Pi)) \subseteq Y^{-1}(\mathcal{T}(\mathbb{A}))$, which is the expected exact translation.

4 Conclusions & Perspectives

In the term rewriting framework, to perform reachability analysis guided by properties of interest, the present paper addresses the question of a systematic translation of linear temporal logic properties into rewrite propositions. More precisely, we have investigated suitable semantics for LTL on maximal rewriting words and their influence on the feasibility of a translation, and proposed a framework providing exact translations on a fragment of LTL corresponding mainly to safety formulæ, and approximations on a larger fragment.

As a future work, we intend to expand the fragment for which translations and approximations can be provided, and study the feasibility of handling equational theories in the same framework. The present work being a part of a rewrite approximation based analysis, the end goal is the integration of the paper's proposals into the verification chain dedicated to the automatic analysis of security-/safety-critical applications.

References

1. Baader, F. (ed.): Term Rewriting and Applications, LNCS, vol. 4533 (2007)
2. Bae, K., Meseguer, J.: The linear temporal logic of rewriting Maude model checker. In: Ölveczky [16], pp. 208–225
3. Boichut, Y., Genet, T., Jensen, T.P., Roux, L.L.: Rewriting approximations for fast prototyping of static analyzers. In: Baader [1], pp. 48–62
4. Boichut, Y., Héam, P.C., Kouchnarenko, O.: Approximation-based tree regular model-checking. Nord. J. Comput. 14(3), 216–241 (2008)
5. Boronat, A., Heckel, R., Meseguer, J.: Rewriting logic semantics and verification of model transformations. In: FASE. LNCS, vol. 5503, pp. 18–33. Springer (2009)
6. Boyer, B., Genet, T.: Verifying Temporal Regular Properties of Abstractions of Term Rewriting Systems. In: RULE. EPTCS, vol. 21, pp. 99–108 (2009)
7. Courbis, R., Héam, P.C., Kouchnarenko, O.: TAGED Approximations for Temporal Properties Model-Checking. In: CIAA. LNCS, vol. 5642. Springer (2009)
8. Dershowitz, N., Jouannaud, J.P.: Rewrite Systems. In: Handbook of Theoretical Computer Science, Volume B: Formal Models and Sematics (B), pp. 243–320 (1990)
9. Escobar, S., Meseguer, J.: Symbolic model checking of infinite-state systems using narrowing. In: Baader [1], pp. 153–168
10. Filiot, E., Talbot, J.M., Tison, S.: Tree automata with global constraints. In: Developments in Language Theory. LNCS, vol. 5257. Springer (2008)

11. Genet, T., Klay, F.: Rewriting for cryptographic protocol verification. In: McAllester, D.A. (ed.) CADE. LNCS, vol. 1831, pp. 271–290. Springer (2000)
12. Kamp, H.W.: Tense Logic and the Theory of Linear Order (1968)
13. Manna, Z., Pnueli, A.: Temporal Verification of Reactive Systems - Safety. Springer (1995)
14. Meseguer, J.: The temporal logic of rewriting: A gentle introduction. In: Concurrency, Graphs and Models. LNCS, vol. 5065. Springer (2008)
15. Meseguer, J.: Conditioned Rewriting Logic as a United Model of Concurrency. TCS 96(1), 73–155 (1992)
16. Ölveczky, P.C. (ed.): Rewriting Logic and Its Applications, LNCS, vol. 6381. Springer (2010)
17. Serbanuta, T.F., Rosu, G., Meseguer, J.: A rewriting logic approach to operational semantics. Inf. Comput. 207(2), 305–340 (2009)

Appendix: Proofs

Lemma 1 [p5]

Proof. **(1)**

$$
\begin{aligned}
(w,i) \models \bigwedge_{m=0}^{\infty} \circ^m \varphi &\iff \bigwedge_{m=0}^{\infty} (w,i) \models \circ^m \varphi \\
&\iff \bigwedge_{m=0}^{\infty} i+m \notin \operatorname{dom} w \vee (w, i+m) \models \varphi \\
&\iff \bigwedge_{m=i}^{\infty} m \notin \operatorname{dom} w \vee (w,m) \models \varphi \\
&\iff \bigwedge_{m=i}^{\#w} (\bot \vee (w,m) \models \varphi) \wedge \bigwedge_{m=1+\#w}^{\infty} (\top \vee (w,m) \models \varphi) \\
&\iff \bigwedge_{m=i}^{\#w} (w,m) \models \varphi \iff \bigwedge_{j=i}^{\#w} (w,j) \models \varphi \\
&\iff \forall j \in \operatorname{dom} w,\ j \geqslant i \Rightarrow (w,j) \models \varphi \\
&\iff (w,i) \models \Box \varphi
\end{aligned}
$$

(2)

$$
\begin{aligned}
(w,i) \models \bigwedge_{m=0}^{\infty} \circ^m \varphi & \\
&\iff (w,i) \models \bigwedge_{m=0}^{k-1} \left(\circ^m \varphi \right) \wedge \bigwedge_{m=k}^{\infty} \left(\circ^m \varphi \right) \\
&\iff (w,i) \models \underbrace{\bigwedge_{m=0}^{k-1} \left(\circ^m \varphi \right)}_{A} \wedge (w,i) \models \bigwedge_{m=k}^{\infty} \left(\circ^m \varphi \right) \\
&\iff \left((w,i) \models A \right) \wedge \bigwedge_{m=k}^{\infty} (w,i) \models \circ^m \varphi \\
&\iff \left((w,i) \models A \right) \wedge \bigwedge_{m=k}^{\infty} \left(i+m \notin \operatorname{dom} w \vee (w, i+m) \models \varphi \right)
\end{aligned}
$$

$$
\begin{aligned}
&\iff \big((w,i) \models A\big) \wedge \bigwedge_{m=0}^{\infty} \Big(i+k+m \notin \operatorname{dom} w \vee (w, i+k+m) \models \varphi\Big) \\
&\iff \big((w,i) \models A\big) \wedge \bigwedge_{m=0}^{\infty} (w, i+k) \models \circ^m \varphi \\
&\iff \big((w,i) \models A\big) \wedge (w, i+k) \models \bigwedge_{m=0}^{\infty} \circ^m \varphi \\
&\iff \big((w,i) \models A\big) \wedge (w, i+k) \models \Box\, \varphi \\
&\iff \big((w,i) \models A\big) \wedge \Big(i+k \notin \operatorname{dom} w \vee (w, i+k) \models \Box\, \varphi\Big) \\
&\iff \big((w,i) \models A\big) \wedge (w, i) \models \circ^k \Box\, \varphi \\
&\iff (w,i) \models A \wedge \circ^k \Box\, \varphi \\
&\iff (w,i) \models \bigwedge_{m=0}^{k-1} \Big(\circ^m \varphi\Big) \wedge \circ^k \Box\, \varphi
\end{aligned}
$$

□

Lemma 2[p9]

Proof. Assume that $i \in \operatorname{dom} w$; the proof is done by induction on $\varphi \in \mathcal{R}$-LTL. Base Cases. Weak and strong semantics are identical by definition except for $\varphi = X$. In that case $(w,i) \models^{s} X \iff w(i) \in X \iff (w,i) \models^{w} X$, because $i \in \operatorname{dom} w$. Inductive Cases. Let $\divideontimes \in \{\wedge, \vee\}$. We have

$$
\begin{aligned}
(w,i) \models^{s} (\varphi \divideontimes \psi) &\iff (w,i) \models^{s} \varphi \ \divideontimes\ (w,i) \models^{s} \psi \\
&\iff (w,i) \models^{w} \varphi \ \divideontimes\ (w,i) \models^{w} \psi \\
&\iff (w,i) \models^{w} (\varphi \divideontimes \psi)\,,
\end{aligned}
$$

the second step being of course by induction hypothesis. Cases $\varphi = \psi \Rightarrow \psi'$, $\varphi = \bullet^m \psi$, $\varphi = \circ^m \psi$ and $\varphi = \Box\, \psi$: weak and strong semantics are identical by definition. □

Lemma 3[p10]

Proof. By induction on the structure of φ. Let us start by noting that $\models^{s}$ is defined in the exact same way as $\models$ in all cases but **(1)** $\varphi = \Box\, \psi$ and **(2)** $\varphi = \circ^m \psi$. This automatically takes care of all those cases, which include the base cases, strong next, material implication, conjunction and disjunction. Now there only remains to deal with the two remaining cases. Let us start by (1) $\varphi = \Box\, \psi$. We have the

induction hypothesis $H \equiv \forall i \in \mathbb{N}_1,\ (w,i) \models^{s} \psi \iff (w,i) \models \psi$. With this in mind, recall that by definition

$$(w,i) \models^{s} \Box\psi \iff \forall j \in \operatorname{dom} w,\ j \geqslant i \Rightarrow (w,j) \models^{w} \psi\ .$$

Since $j \in \operatorname{dom} w$, by the previous lemma we have $(w,j) \models^{s} \psi \Leftrightarrow (w,j) \models^{w} \psi$ and can effect this replacement in the formula:

$$(w,i) \models^{s} \Box\psi \iff \forall j \in \operatorname{dom} w,\ j \geqslant i \Rightarrow (w,j) \models^{s} \psi\ .$$

There remains to recall our hypothesis $H, : \forall j,\ (w,j) \models^{s} \psi \iff (w,j) \models \psi$:

$$\begin{aligned}(w,i) \models^{s} \Box\psi &\iff \forall j \in \operatorname{dom} w,\ j \geqslant i \Rightarrow (w,j) \models \psi \\ &\iff (w,i) \models \Box\psi\ ,\end{aligned}$$

which concludes the proof for case (1). Now we deal with (2) $\varphi = \circ^{m}\psi$, using the same arguments.

$$\begin{aligned}(w,i) \models^{s} \circ^{m}\varphi &\iff i+m \notin \operatorname{dom} w \vee (w,i+m) \models^{w} \varphi \\ &\iff i+m \in \operatorname{dom} w \implies (w,i+m) \models^{w} \varphi \\ &\iff i+m \in \operatorname{dom} w \implies (w,i+m) \models^{s} \varphi \\ &\iff i+m \in \operatorname{dom} w \implies (w,i+m) \models \varphi \\ &\iff (w,i) \models \circ^{m}\varphi\ .\end{aligned}$$

□

Remark 4[p10]

Proof. The associativity and commutativity of $\otimes$ stem directly from those of $\cup$ and $\cap$. The neutrality of $\varepsilon = \{\!|\mathcal{R} \mid \overline{\mathbb{N}}|\!\}$ stems from that of $\overline{\mathbb{N}}$ $(= \nabla\varepsilon)$ for $\cap$ within $\wp(\overline{\mathbb{N}})$, of $\mathcal{R}$ $(= \varepsilon[k]\ , \forall k)$ for $\cap$ within $\wp(\mathcal{R})$, and of $\varnothing$ (its domain) for $\cup$. □

Lemma 7[p12]

Proof. **(1)** For all $n \in \mathbb{N}$, $\nabla\rho_n = \bigcap_{i=0}^{n} \nabla\sigma_i$, thus it is clear that $\nabla\rho_n = \bigcap_{i=0}^{n} \nabla\sigma_i \supseteq \bigcap_{i=0}^{n+1} \nabla\sigma_i = \nabla\rho_{n+1}$ or, in other words, $(\nabla\rho_n)_{n\in\mathbb{N}}$ is a (trivial) contracting sequence of finite sets. Therefore it converges towards $\bigcap_{i=0}^{\infty} \nabla\sigma_i$. **(2)** Let $k \in \mathbb{N}_1$; we have

$$\rho_n[k] = \left(\bigotimes_{i=0}^{n} \sigma_i\right)[k] = \bigcap_{i=0}^{n} \sigma_i[k]\ ,$$

and thus $\rho_n[k] = \bigcap_{i=0}^{n} \sigma_i[k] \supseteq \bigcap_{i=0}^{n+1} \sigma_i[k] = \rho_{n+1}[k]$ and again, $(\rho_n[k])_{n\in\mathbb{N}}$ is a trivial contracting sequence of finite sets; therefore it converges towards a limit which we denote by $\rho_\infty[k] = \bigcap_{i=0}^{\infty} \sigma_i[k]$. **(3)** Suppose now that $\sigma_i = \sigma \triangleright i$ (resp. $\sigma_i = \sigma \blacktriangleright i$, the computation will be unchanged), we have

$$\begin{aligned}\rho_\infty[k] = \bigcap_{i=0}^{\infty} \sigma_i[k] = \bigcap_{i=0}^{\infty} (\sigma \triangleright i)[k] &= \left(\bigcap_{i=0}^{k-1} (\sigma \triangleright i)[k]\right) \cap \left(\bigcap_{i=k}^{\infty} (\sigma \triangleright i)[k]\right) \\ &= \left(\bigcap_{i=0}^{k-1} \sigma[k-i]\right) \cap \left(\bigcap_{i=k}^{\infty} \mathcal{R}\right) = \bigcap_{i=0}^{k-1} \sigma[k-i] = \bigcap_{i=1}^{k} \sigma[i] \,.\end{aligned}$$

Given that for all $i > \#\sigma$, $\sigma[i] = \sigma[\omega]$, it follows that for all $k > \#\sigma$, $\rho_\infty[k] = \bigcap_{i=1}^{\#\sigma+1} \sigma[i]$. Thus $(\rho_\infty[k])_{k\in\mathbb{N}_1}$ converges. This shows that the infinite product $\bigotimes_{n=0}^{\infty} \sigma_n$ is convergent. □

Lemma 5[p11]

Proof.

$$\begin{aligned}{}^{\mathcal{R}}(\!|\Pi \fatsemi \varepsilon|\!) &= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\varepsilon \;\wedge\; \forall k \in \operatorname{dom} w,\ w(k) \in \varepsilon[k] \right\} \\ &= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \overline{\mathbb{N}} \;\wedge\; \forall k \in \operatorname{dom} w,\ w(k) \in \mathcal{R} \right\} \\ &= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \top \;\wedge\; \top \right\} = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \top \right\} = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \top \right\} \\ &= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \right\} = {}^{\mathcal{R}}(\!|\Pi|\!) \,.\end{aligned}$$

□

Lemma 6[p11]

Proof. **(1)** Let $\rho = \sigma \otimes \sigma'$. ${}^{\mathcal{R}}(\!|\Pi \fatsemi \rho|\!) = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\rho \wedge \forall k \in \operatorname{dom} w, w(k) \in \rho[k] \right\}$. Let us rewrite this condition using the definition of ρ:

$$\begin{aligned}&\#w \in \nabla\rho \wedge \forall k \in \operatorname{dom} w, w(k) \in \rho[k] \\ \iff &\#w \in \nabla\sigma \cap \nabla\sigma' \wedge \forall k \in \operatorname{dom} w, w(k) \in \sigma[k] \cap \sigma'[k] \\ \iff &\#w \in \nabla\sigma \wedge \forall k \in \operatorname{dom} w, w(k) \in \sigma[k] \\ &\quad \wedge \#w \in \nabla\sigma' \wedge \forall k \in \operatorname{dom} w, w(k) \in \sigma'[k] \\ \iff &w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \wedge w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma'|\!) \\ \iff &w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \cap {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma'|\!) \,,\end{aligned}$$

therefore

$${}^{\mathcal{R}}(\!|\Pi \fatsemi \rho|\!) = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \cap {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma'|\!) \right\}$$

$$= {}^{\mathcal{R}}(\!|\Pi|\!) \cap {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \cap {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma'|\!)$$
$$= {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \cap {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma'|\!) \ .$$

(2) Let $\rho_\infty = \bigotimes_{n=0}^{\infty} \sigma_n$. We have

$$\begin{aligned}
{}^{\mathcal{R}}(\!|\Pi \fatsemi \rho_\infty|\!) &= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_\infty \wedge \forall k \in \operatorname{dom} w, w(k) \in \rho_\infty[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \bigcap_{n=0}^{\infty} \nabla\sigma_n \wedge \forall k \in \operatorname{dom} w, w(k) \in \rho_\infty[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \bigcap_{n=0}^{\infty} \nabla\sigma_n \wedge \forall k \in \operatorname{dom} w, w(k) \in \bigcap_{n=0}^{\infty} \sigma_n[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \bigwedge_{n=0}^{\infty} \left(\#w \in \nabla\sigma_n\right) \wedge \forall k \in \operatorname{dom} w, \bigwedge_{n=0}^{\infty} w(k) \in \sigma_n[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \bigwedge_{n=0}^{\infty} \left(\#w \in \nabla\sigma_n \wedge \forall k \in \operatorname{dom} w, w(k) \in \sigma_n[k]\right) \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \bigwedge_{n=0}^{\infty} w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma_n|\!) \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \in \bigcap_{n=0}^{\infty} {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma_n|\!) \right\} = \bigcap_{n=0}^{\infty} {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma_n|\!) \ .
\end{aligned}$$

□

Lemma 13[p14]

Proof. **(1 : ⊆)** Let $x \in {}^{\mathcal{R}}(\!|\Pi_\sigma^m \fatsemi \sigma \lhd m|\!)$. There exists $u_m \in \Pi_\sigma^m$ such that $u_m \xrightarrow{x(1)} u_{m+1} \xrightarrow{x(2)} u_{m+2} \xrightarrow{x(3)} \cdots$, and $u_{m+\#x} \notin \mathcal{R}^{-1}(\mathcal{T}(\mathbb{A}))$. By definition of Π_σ^m, there exist $u_0, \ldots, u_{m-1} \in \mathcal{T}(\mathbb{A})$ such that $u_0 \in \Pi_\sigma^0 = \Pi, \ldots, u_{m-1} \in \Pi_\sigma^{m-1}$ and $\rho_1, \ldots, \rho_m \in \mathcal{R}$ such that $\rho_1 \in \sigma[1], \ldots, \rho_m \in \sigma[m]$ and $u_0 \xrightarrow{\rho_1} u_1 \xrightarrow{\rho_2} \cdots \xrightarrow{\rho_m} u_m$. Let us consider the word $w = \rho_1 \ldots \rho_m x$; its length is $\#w = \#x + m$ and $\#x \in \nabla(\sigma \lhd m) = \nabla\sigma - m$, thus $\#w \in (\nabla\sigma - m) + m = \nabla\sigma \setminus [\![0, m-1]\!]$. Furthermore, for all $k \in [\![1, m]\!]$, we have by construction $w(k) = \rho_k \in \sigma[k]$, and for all $k \in [\![m+1, \#w]\!]$, $w(k) = x(k-m)$. By definition of $x \in {}^{\mathcal{R}}(\!|\Pi_\sigma^m \fatsemi \sigma \lhd m|\!)$, for all $i \in \operatorname{dom} x$, $x(i) \in (\sigma \lhd m)[i] = \sigma[i+m]$, thus for all $k \in [\![m+1, \#w]\!]$, $w(k) = x(k-m) \in \sigma[k-m+m] = \sigma[k-m+m] = \sigma[k]$. So we have that for all $k \in \operatorname{dom} w$, $w(k) \in \sigma[k]$. Thus we have built a word $w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \wr \partial\sigma \mid \nabla\sigma \setminus [\![0, m-1]\!] \wr|\!)$ such that $w^{m+1} = x$. There only remains to remark that $w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \wr \partial\sigma \mid \nabla\sigma \setminus [\![0, m-1]\!] \wr|\!) \iff w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \wedge \#w \geqslant m$, and

we can conclude this part. **(2 : ⊇)** Let $x \in \left\{ w^{m+1} \;\middle|\; w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \wedge \#w \geqslant m \right\}$, and let $w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!)$ such that $x = w^{m+1}$; by the same type of immediate arguments as for (1), $x \in {}^{\mathcal{R}}(\!|\Pi^m_\sigma|\!)$. For all $k \in \operatorname{dom} w$, $w(k) \in \sigma[k]$, so for all $k \in \operatorname{dom} x$, $x(k) = w^{m+1}(k) = w(k+m) \in \sigma[k+m] = (\sigma \lhd m)[k]$. As above, we have $\#w \in \nabla\sigma \setminus [\![0, m-1]\!]$, and since $\#x = \#w - m$, it follows that $\#x \in (\nabla\sigma \setminus [\![0, m-1]\!]) - m = (\nabla\sigma - m) \cap \overline{\mathbb{N}} = \nabla(\sigma \lhd m)$. Thus $x \in {}^{\mathcal{R}}(\!|\Pi^m_\sigma \fatsemi \sigma \lhd m|\!)$. □

Lemma 11[p14]

Proof. Let us start by noting that the statements $(\#w \neq n)$ and $(\#w \geqslant n \Rightarrow \#w > n)$ are equivalent, and keeping in mind that if $w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!)$ is of length n, we have $u_0 \xrightarrow{w(1)} u_1 \xrightarrow{w(2)} \cdots \xrightarrow{w(n)} u_n$, with $u_0 \in \Pi^0_\sigma = \Pi$ and $u_n \in \Pi^n_\sigma$. This said, $\Psi^\sigma_\Pi(n)$ holds by definition if and only if $\Pi^n_\sigma \subseteq \sigma[n+1]^{-1}(\mathcal{T}(\mathbb{A}))$, which is the formal way of saying "any term in Π^n_σ can be rewritten by a rule in $\sigma[n+1]$". It is equivalent to saying that for any $w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!)$, if $n \in \operatorname{dom} w$, then $n+1 \in \operatorname{dom} w$, because only the *maximal* rewrite words are in ${}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!)$. In other words, $\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!)$, $\#w \geqslant n \Rightarrow \#w \geqslant n+1$, or even more simply, $\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!)$, $\#w \neq n$. □

Corollary 12[p14]

Proof. By Lemma 11[p14], we have immediately

$$\begin{aligned}
\bigwedge_{n \in S \cap \nabla\sigma} \Psi^\sigma_\Pi(n) &\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \#w \notin S \cap \nabla\sigma \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \#w \notin S \vee \#w \notin \nabla\sigma \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \#w \notin S \vee \bot \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \#w \notin S\ .
\end{aligned}$$

□

Remark 14[p14]

Proof. It is immediate from the definition that we have $\bigcup_{i \in I} {}^{\mathcal{R}}(\!|\Pi_i|\!) = {}^{\mathcal{R}}(\!|\bigcup_{i \in I} \Pi_i|\!)$. Likewise, we have by definition ${}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; P(w, \sigma) \right\}$, where $P(w, \sigma)$ is some predicate depending only on on w and σ, the details of which are irrelevant for this proof. We have $\bigcup_{i \in I} {}^{\mathcal{R}}(\!|\Pi_i \fatsemi \sigma|\!) = \bigcup_{i \in I} \left\{ w \in {}^{\mathcal{R}}(\!|\Pi_i|\!) \;\middle|\; P(w, \sigma) \right\} = \left\{ w \in \bigcup_{n \in I} {}^{\mathcal{R}}(\!|\Pi_i|\!) \;\middle|\; P(w, \sigma) \right\} = \left\{ w \in {}^{\mathcal{R}}(\!|\bigcup_{n \in I} \Pi_i|\!) \;\middle|\; P(w, \sigma) \right\} = {}^{\mathcal{R}}(\!|\bigcup_{n \in I} \Pi_i \fatsemi \sigma|\!)$. □

Lemma 15[p15]

Proof. Using Lemma 13[p14].

$$\begin{aligned}
&\left\{ w^{1+n} \;\middle|\; n \in \mathbb{N},\ w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \#w \geqslant n \right\} \\
&\quad = \bigcup_{n=0}^{\infty} \left\{ w^{1+n} \;\middle|\; w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \#w \geqslant n \right\} \\
&\quad = \bigcup_{n=0}^{\infty} {}^{\mathcal{R}}(\!|\Pi^n_\sigma \fatsemi \sigma \lhd n|\!) = \bigcup_{n=0}^{\infty} {}^{\mathcal{R}}(\!|\Pi^n_\sigma \fatsemi \sigma|\!) = {}^{\mathcal{R}}(\!|\bigcup_{n=0}^{\infty} \Pi^n_\sigma \fatsemi \sigma|\!) \\
&\quad = {}^{\mathcal{R}}(\!|\bigcup_{n=0}^{\infty} \sigma[\omega]^n\,(\Pi) \fatsemi \sigma|\!) = {}^{\mathcal{R}}(\!|\sigma[\omega]^*\,(\Pi) \fatsemi \sigma|\!)\ .
\end{aligned}$$

□

Theorem 8[p13]

Proof. By induction on the structure of φ. Case $\sigma = \xi(\top)$:

$$ {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\top)|\!) = {}^{\mathcal{R}}(\!|\Pi \fatsemi \varepsilon|\!) = {}^{\mathcal{R}}(\!|\Pi|\!) = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \top \right\}\ . $$

Case $\sigma = \xi(\bot)$:

$$\begin{aligned}
&{}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\bot)|\!) = {}^{\mathcal{R}}(\!|\Pi \fatsemi (\!|\varnothing \mid \varnothing|\!)|\!) \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma \wedge \forall k \in \operatorname{dom} w, w(k) \in \sigma[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \varnothing \wedge \forall k \in \operatorname{dom} w, w(k) \in \varnothing \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \bot \wedge \bot \right\} = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \bot \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \bot \right\}
\end{aligned}$$

Case $\sigma = \xi(X)$:

$$\begin{aligned}
&{}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(X)|\!) = {}^{\mathcal{R}}(\!|\Pi \fatsemi (\!|X \fatsemi \mathcal{R} \mid \overline{\mathbb{N}}_1|\!)|\!) \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma \wedge \forall k \in \operatorname{dom} w, w(k) \in \sigma[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \geqslant 1 \wedge w(1) \in X \wedge \forall k \in \operatorname{dom} w, k > 1 \Rightarrow w(k) \in \sigma[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; 1 \in \operatorname{dom} w \wedge w(1) \in X \wedge \forall k \in \operatorname{dom} w, k > 1 \Rightarrow w(k) \in \mathcal{R} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; 1 \in \operatorname{dom} w \wedge w(1) \in X \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; (w, 1) \models X \right\} = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models X \right\}
\end{aligned}$$

Case $\sigma = \xi(\neg X)$:

$$ {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\neg X)|\!) = {}^{\mathcal{R}}(\!|\Pi \fatsemi (\!|\mathcal{R} \setminus X \fatsemi \mathcal{R} \mid \overline{\mathbb{N}}|\!)|\!) $$

$$
\begin{aligned}
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma \wedge \forall k \in \operatorname{dom} w, w(k) \in \sigma[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \overline{\mathbb{N}} \wedge \forall k \in \operatorname{dom} w, w(k) \in \sigma[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \top \wedge \forall k \in \operatorname{dom} w, w(k) \in \sigma[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \forall k \in \operatorname{dom} w, w(k) \in \sigma[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} 1 \in \operatorname{dom} w \Rightarrow w(1) \in \mathcal{R} \setminus X \quad \wedge \\ \forall k \in \operatorname{dom} w, k > 1 \Rightarrow w(k) \in \sigma[k] \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} 1 \in \operatorname{dom} w \Rightarrow w(1) \in \mathcal{R} \setminus X \quad \wedge \\ \forall k \in \operatorname{dom} w, k > 1 \Rightarrow w(k) \in \mathcal{R} \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; 1 \in \operatorname{dom} w \Rightarrow w(1) \in \mathcal{R} \setminus X \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; 1 \notin \operatorname{dom} w \vee w(1) \in \mathcal{R} \setminus X \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; 1 \notin \operatorname{dom} w \vee w(1) \notin X \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \neg X \right\}
\end{aligned}
$$

Case $\sigma = \xi(X \wedge Y)$: In the first steps, we successively use the definition of the signature, the signature-product lemma, and the induction hypothesis.

$$
\begin{aligned}
{}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi \wedge \psi)|\!) &= {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi) \otimes \xi(\psi)|\!) \\
&= {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi)|\!) \cap {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\psi)|\!) \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \varphi \right\} \cap \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \psi \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \psi \wedge w \models \varphi \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \psi \wedge \varphi \right\}
\end{aligned}
$$

Case $\xi(\bullet^m \varphi) = \xi(\varphi) \blacktriangleright m$: For simplicity of notation, let $\sigma \triangleq \xi(\varphi)$ and $\sigma_m = \xi(\varphi) \blacktriangleright m$. By induction hypothesis we have ${}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi)|\!) = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \varphi \right\}$. Let us note before beginning that $\#w \in \nabla\sigma_m$ implies that $\#w > m$. We have:

$$
\begin{aligned}
&{}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\bullet^m \varphi)|\!) \\
&= {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi) \blacktriangleright m|\!) = {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma \blacktriangleright m|\!) = {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma_m|\!) \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_m \;\wedge\; \forall k \in \operatorname{dom} w,\; w(k) \in \sigma_m[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_m \;\wedge\; \forall 1 \leqslant k \leqslant \#w,\; w(k) \in \sigma_m[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_m \;\wedge\; \left| \begin{array}{l} \forall 1 \leqslant k \leqslant m,\; w(k) \in \sigma_m[k] \\ \forall m+1 \leqslant k \leqslant \#w,\; w(k) \in \sigma_m[k] \end{array} \right. \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_m \;\wedge\; \left| \begin{array}{l} \forall 1 \leqslant k \leqslant m,\; w(k) \in \mathcal{R} \\ \forall m+1 \leqslant k \leqslant \#w,\; w(k) \in \sigma_m[k] \end{array} \right. \right\}
\end{aligned}
$$

$$
\begin{aligned}
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_m \;\wedge\; \forall m+1 \leqslant k \leqslant \#w,\; w(k) \in \sigma_m[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_m \;\wedge\; \forall m+1 \leqslant k \leqslant \#w,\; w(k) \in \sigma[k-m] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} \#w \in \nabla\sigma_m \wedge \\ \forall 1 \leqslant k-m \leqslant \#w-m,\; w(k-m+m) \in \sigma[k-m] \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_m \;\wedge\; \forall 1 \leqslant k \leqslant \#w-m,\; w(k+m) \in \sigma[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_m \;\wedge\; \forall 1 \leqslant k \leqslant \#w^{m+1},\; w^{m+1}(k) \in \sigma[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_m \;\wedge\; \forall k \in \operatorname{dom} w^{m+1},\; w^{m+1}(k) \in \sigma[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} \#w \in (\nabla\sigma \setminus \{0\}) + m \wedge \\ \forall k \in \operatorname{dom} w^{m+1},\; w^{m+1}(k) \in \sigma[k] \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} \#w^{m+1} + m \in (\nabla\sigma \setminus \{0\}) + m \wedge \\ \forall k \in \operatorname{dom} w^{m+1},\; w^{m+1}(k) \in \sigma[k] \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} \#w^{m+1} \in (\nabla\sigma \setminus \{0\}) \wedge \\ \forall k \in \operatorname{dom} w^{m+1},\; w^{m+1}(k) \in \sigma[k] \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} \#w^{m+1} \neq 0 \wedge \#w^{m+1} \in \nabla\sigma \wedge \\ \forall k \in \operatorname{dom} w^{m+1},\; w^{m+1}(k) \in \sigma[k] \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} m+1 \in \operatorname{dom} w \wedge \#w^{m+1} \in \nabla\sigma \wedge \\ \forall k \in \operatorname{dom} w^{m+1},\; w^{m+1}(k) \in \sigma[k] \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; m+1 \in \operatorname{dom} w \wedge w^{m+1} \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; m+1 \in \operatorname{dom} w \wedge w^{m+1} \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi)|\!) \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; m+1 \in \operatorname{dom} w \wedge w^{m+1} \in \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \varphi \right\} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; m+1 \in \operatorname{dom} w \wedge w^{m+1} \models \varphi \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; m+1 \in \operatorname{dom} w \wedge (w, m+1) \models \varphi \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; (w,1) \models \bullet^m \varphi \right\} = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \bullet^m \varphi \right\} .
\end{aligned}
$$

Case $\xi(\circ^m \varphi) = \xi(\varphi) \rhd m$: For simplicity of notation, let $\sigma \triangleq \xi(\varphi)$ and $\sigma_m = \xi(\varphi) \rhd m$. By induction hypothesis we have ${}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi)|\!) = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \varphi \right\}$. Note that we will reuse steps from the strong case, as the two proofs are very similar. Indeed they only differ where $\nabla\sigma_m$ is concerned. We have:

$$
\begin{aligned}
&{}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\circ^m \varphi)|\!) \\
&= {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi) \rhd m|\!) = {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma \rhd m|\!) = {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma_m|\!) \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_m \;\wedge\; \forall k \in \operatorname{dom} w,\; w(k) \in \sigma_m[k] \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w \in \nabla\sigma_m \;\wedge\; \forall k \in \operatorname{dom} w^{m+1},\; w^{m+1}(k) \in \sigma[k] \right\}
\end{aligned}
$$

$$
\begin{aligned}
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} \#w \in [\![0, m]\!] \cup (\nabla\sigma + m) \wedge \\ \forall k \in \operatorname{dom} w^{m+1},\ w^{m+1}(k) \in \sigma[k] \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} (\#w < m+1 \vee \#w \in \nabla\sigma + m) \wedge \\ \forall k \in \operatorname{dom} w^{m+1},\ w^{m+1}(k) \in \sigma[k] \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} (\#w < m+1 \vee \#w^{m+1} + m \in \nabla\sigma + m) \wedge \\ \forall k \in \operatorname{dom} w^{m+1},\ w^{m+1}(k) \in \sigma[k] \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} (\#w < m+1 \vee \#w^{m+1} \in \nabla\sigma) \wedge \\ \forall k \in \operatorname{dom} w^{m+1},\ w^{m+1}(k) \in \sigma[k] \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} (\#w < m+1 \wedge \forall k \in \operatorname{dom} w^{m+1},\ w^{m+1}(k) \in \sigma[k]) \\ \vee (\#w^{m+1} \in \nabla\sigma \wedge \forall k \in \operatorname{dom} w^{m+1},\ w^{m+1}(k) \in \sigma[k]) \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} (\#w < m+1 \wedge \forall k \in \varnothing,\ w^{m+1}(k) \in \sigma[k]) \\ \vee (\#w^{m+1} \in \nabla\sigma \wedge \forall k \in \operatorname{dom} w^{m+1},\ w^{m+1}(k) \in \sigma[k]) \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \begin{array}{l} \#w < m+1 \\ \vee (\#w^{m+1} \in \nabla\sigma \wedge \forall k \in \operatorname{dom} w^{m+1},\ w^{m+1}(k) \in \sigma[k]) \end{array} \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; \#w < m+1 \vee (w, m+1) \models \varphi \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; m+1 \notin \operatorname{dom} w \vee (w, m+1) \models \varphi \right\} \\
&= \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \circ^m \varphi \right\} .
\end{aligned}
$$

Case $\xi(\Box\,\varphi) = \bigotimes_{m=0}^{\infty} \left[\xi(\varphi) \rhd m\right]$. Let us start by noting that, by application of the product-breaking lemma, we have ${}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\Box\,\varphi)|\!) = {}^{\mathcal{R}}(\!|\Pi \fatsemi \bigotimes_{m=0}^{\infty} \xi(\varphi) \rhd m|\!) = \bigcap_{m=0}^{\infty} {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi) \rhd m|\!)$. Let $w \in {}^{\mathcal{R}}(\!|\Pi|\!)$; we have

$$
\begin{aligned}
w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\Box\,\varphi)|\!) &\iff w \in \bigcap_{m=0}^{\infty} {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi) \rhd m|\!) \\
&\iff \bigwedge_{m=0}^{\infty} w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi) \rhd m|\!) \\
&\iff \bigwedge_{m=0}^{\infty} w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\circ^m \varphi)|\!) \\
&\iff \bigwedge_{m=0}^{\infty} w \models \circ^m \varphi \iff w \models \bigwedge_{m=0}^{\infty} \circ^m \varphi \\
&\iff w \models \Box\,\varphi ,
\end{aligned}
$$

the last step being by lemma 1[p5]. So we have finally ${}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\Box\,\varphi)|\!) = \left\{ w \in {}^{\mathcal{R}}(\!|\Pi|\!) \;\middle|\; w \models \Box\,\varphi \right\}$. □

Proposition 16[p15]

Proof. By induction on φ. □

Theorem 9[p14]

Proof. Recall that the no-constraints lemma states that ${}^{\mathcal{R}}(\!|\Pi \fatsemi \varepsilon|\!) = {}^{\mathcal{R}}(\!|\Pi|\!)$. Keeping the Strong Semantics Lemma in mind as well, we have immediately

$$\begin{aligned}
\langle \Pi \fatsemi \varepsilon \;\Vdash^{\mathbf{s}}\; \varphi \rangle &\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \varepsilon|\!),\ w \models^{\mathbf{s}} \varphi \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi|\!),\ w \models^{\mathbf{s}} \varphi \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi|\!),\ w \models \varphi \\
&\iff \mathcal{R}, \Pi \models \varphi\ .
\end{aligned}$$

□

Remark 10[p14]

Proof.

$$\begin{aligned}
\langle \Pi \fatsemi \sigma \;\Vdash^{\mu}\; \Box\varphi \rangle &\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \Box\varphi \\
&\iff (\lambda \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \star\sigma|\!) \Rightarrow \lambda \models^{\mu} \Box\varphi) \wedge \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \star\sigma|\!),\ w \models^{\mu} \Box\varphi \\
&\iff (\lambda \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \star\sigma|\!) \Rightarrow \top) \wedge \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \star\sigma|\!),\ w \models^{\mu} \Box\varphi \\
&\iff \top \wedge \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \star\sigma|\!),\ w \models^{\mu} \Box\varphi \\
&\iff \langle \Pi \fatsemi \star\sigma \;\Vdash^{\mu}\; \Box\varphi \rangle\ .
\end{aligned}$$

□

Proofs of translation rules.

Proof of rules $(\top)_{[p15]}$ *and* $(\bot)$. For all Π, σ, μ:

$$\begin{aligned}
\langle \Pi \fatsemi \sigma \;\Vdash^{\mu}\; \top \rangle &\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \top \\
&\iff \top
\end{aligned}$$

$$\begin{aligned}
\langle \Pi \fatsemi \sigma \;\Vdash^{\mu}\; \bot \rangle &\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \bot \\
&\iff \bot
\end{aligned}$$

□

Proof of rule $(\wedge_X)_{[p15]}$. Let us first assume that w is not the empty word, that is to say, $1 \in \operatorname{dom} w$; then $w \models^{\mathbf{s}} X \iff w \models^{\mathbf{w}} X \iff w(1) \in X$ and we have, for all Π, σ, μ:

$$\begin{aligned}
\langle \Pi \fatsemi \sigma \Vdash^{\mu} X \wedge Y \rangle &\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} X \wedge Y \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} X \wedge Y \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ (w \models^{\mu} X) \wedge (w \models^{\mu} Y) \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ (w(1) \in X) \wedge (w(1) \in Y) \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w(1) \in X \cap Y \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} X \cap Y \\
&\iff \langle \Pi \fatsemi \sigma \Vdash^{\mu} X \cap Y \rangle
\end{aligned}$$

Now, if w is the empty word, we have

$$\begin{aligned}
\langle \Pi \fatsemi \sigma \Vdash^{\mathbf{s}} X \wedge Y \rangle &\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mathbf{s}} X \wedge Y \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mathbf{s}} X \wedge Y \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ (w \models^{\mathbf{s}} X) \wedge (w \models^{\mathbf{s}} Y) \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \bot \wedge \bot \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \bot \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mathbf{s}} X \cap Y \\
&\iff \langle \Pi \fatsemi \sigma \Vdash^{\mathbf{s}} X \cap Y \rangle
\end{aligned}$$

$$\begin{aligned}
\langle \Pi \fatsemi \sigma \Vdash^{\mathbf{w}} X \wedge Y \rangle &\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mathbf{w}} X \wedge Y \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mathbf{w}} X \wedge Y \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ (w \models^{\mathbf{w}} X) \wedge (w \models^{\mathbf{w}} Y) \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \top \wedge \top \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \top \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mathbf{w}} X \cap Y \\
&\iff \langle \Pi \fatsemi \sigma \Vdash^{\mathbf{w}} X \cap Y \rangle
\end{aligned}$$

The proof of $(\vee_X)_{[p15]}$ is the same, with the substitution $\vee/\wedge$, $\cup/\cap$. □

Proof of rule $(\wedge)_{[p15]}$.

$$\langle \Pi \fatsemi \sigma \Vdash^{\mu} \varphi \wedge \psi \rangle$$

$$
\begin{aligned}
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \varphi \wedge \psi \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \varphi \wedge w \models^{\mu} \psi \\
&\iff \big(\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \varphi\big) \wedge \big(\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \psi\big) \\
&\iff \langle \Pi \fatsemi \sigma \ \Vdash^{\mu}\ \varphi\rangle \wedge \langle \Pi \fatsemi \sigma \ \Vdash^{\mu}\ \psi\rangle
\end{aligned}
$$

□

Proof of rule $(\vee_{\uparrow})_{[p15]}$.

$$
\begin{aligned}
&\langle \Pi \fatsemi \sigma \ \Vdash^{\mu}\ \varphi\rangle \vee \langle \Pi \fatsemi \sigma \ \Vdash^{\mu}\ \psi\rangle \\
\implies &\big(\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \varphi\big) \vee \big(\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \psi\big) \\
\implies &\big(\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \varphi \vee \psi\big) \vee \big(\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \varphi \vee \psi\big) \\
\implies &\big(\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \varphi \vee \psi\big) \\
\implies &\langle \Pi \fatsemi \sigma \ \Vdash^{\mu}\ \varphi \vee \psi\rangle
\end{aligned}
$$

□

Proof of rule $(\vee^{\neg}_{\Rightarrow})_{[p15]}$. Obvious by $\varphi \vee \psi \iff \neg\varphi \Rightarrow \psi$. The only snag is that $\neg\varphi$ is not necessarily an $\mathcal{A}$-LTL formula and thus its signature may not exist. In that case the rule cannot be invoked. □

Proof of rule $(\vee^{\Rightarrow}_{\wedge})_{[p15]}$.

$$
\begin{aligned}
&\langle \Pi \fatsemi \sigma \ \Vdash^{\mu}\ [\varphi \vee \varphi'] \Rightarrow \psi\rangle \\
\iff &\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} [\varphi \vee \varphi'] \Rightarrow \psi \\
\iff &\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} (\varphi \Rightarrow \psi) \wedge (\varphi' \Rightarrow \psi) \\
\iff &\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ (w \models^{\mu} \varphi \Rightarrow \psi) \wedge (w \models^{\mu} \varphi' \Rightarrow \psi) \\
\iff &\big(\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \varphi \Rightarrow \psi\big) \wedge \big(\forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \varphi' \Rightarrow \psi\big) \\
\iff &\langle \Pi \fatsemi \sigma \ \Vdash^{\mu}\ \varphi \Rightarrow \psi\rangle \wedge \langle \Pi \fatsemi \sigma \ \Vdash^{\mu}\ \varphi' \Rightarrow \psi\rangle
\end{aligned}
$$

□

Proof of rule $(\Rightarrow_{\Sigma})_{[p15]}$.

$$
\begin{aligned}
\langle \Pi \fatsemi \sigma \ \Vdash^{\mu}\ \varphi \Rightarrow \psi\rangle &\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \varphi \Rightarrow \psi \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ (w \models^{\mathbf{s}} \varphi) \Rightarrow (w \models^{\mathbf{s}} \psi) \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ (w \models \varphi) \Rightarrow (w \models^{\mathbf{s}} \psi) \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ (w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi)|\!)) \Rightarrow (w \models^{\mathbf{s}} \psi)
\end{aligned}
$$

$$\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!) \cap {}^{\mathcal{R}}(\!|\Pi \fatsemi \xi(\varphi)|\!),\ w \models^{\mathbf{s}} \psi$$
$$\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma \otimes \xi(\varphi)|\!),\ w \models^{\mathbf{s}} \psi$$
$$\iff \langle \Pi \fatsemi \sigma \otimes \xi(\varphi) \ \Vdash^{\mathbf{s}} \ \psi \rangle$$

□

Proof of rule $(\circ^{m})_{[p15]}$. We use Lemma 13$_{[p14]}$.

$$\begin{aligned}
&\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \circ^{m}\varphi \rangle \\
&\quad\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \circ^{m}\varphi \\
&\quad\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ 1+m \notin \operatorname{dom} w \vee (w, 1+m) \models^{\mathbf{w}} \varphi \\
&\quad\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \#w \geqslant 1+m \implies w^{1+m} \models^{\mathbf{w}} \varphi \\
&\quad\iff \forall x \in {}^{\mathcal{R}}(\!|\Pi^{m}_{\sigma} \fatsemi \sigma \lhd m|\!),\ \#x + m \geqslant 1+m \implies x \models^{\mathbf{w}} \varphi \\
&\quad\iff \forall x \in {}^{\mathcal{R}}(\!|\Pi^{m}_{\sigma} \fatsemi \sigma \lhd m|\!),\ \#x \geqslant 1 \implies x \models^{\mathbf{w}} \varphi \\
&\quad\iff \forall x \in {}^{\mathcal{R}}(\!|\Pi^{m}_{\sigma} \fatsemi \sigma \blacktriangleleft m|\!),\ x \models^{\mathbf{w}} \varphi \\
&\quad\iff \langle \Pi^{m}_{\sigma} \fatsemi \sigma \blacktriangleleft m \ \Vdash^{\mathbf{w}} \ \varphi \rangle\ .
\end{aligned}$$

□

Proof of rule $(\bullet^{m})_{[p15]}$. We use Corollary 12$_{[p14]}$, as well as Lemma 2$_{[p9]}$.

$$\begin{aligned}
&\langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \bullet^{m}\varphi \rangle \\
&\quad\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \bullet^{m}\varphi \\
&\quad\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ 1+m \in \operatorname{dom} w \wedge (w, 1+m) \models^{\mathbf{s}} \varphi \\
&\quad\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \#w > m \wedge (w, 1+m) \models^{\mathbf{s}} \varphi \\
&\quad\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \#w > m \wedge (1+m \in \operatorname{dom} w \Rightarrow (w, 1+m) \models^{\mathbf{s}} \varphi) \\
&\quad\iff \begin{cases} \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \#w > m \\ \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ (1+m \in \operatorname{dom} w \Rightarrow (w, 1+m) \models^{\mathbf{s}} \varphi) \end{cases} \\
&\quad\iff \begin{cases} \bigwedge_{n \in [\![0,m]\!] \cap \nabla\sigma} \Psi^{\sigma}_{\Pi}(n) \\ \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ (1+m \in \operatorname{dom} w \Rightarrow (w, 1+m) \models^{\mathbf{w}} \varphi) \end{cases} \\
&\quad\iff \begin{cases} \bigwedge_{n \in [\![0,m]\!] \cap \nabla\sigma} \Psi^{\sigma}_{\Pi}(n) \\ \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \circ^{m}\varphi \end{cases} \\
&\quad\iff \langle \Pi \fatsemi \sigma \ \Vdash^{\mu} \ \circ^{m}\varphi \rangle \wedge \bigwedge_{n \in [\![0,m]\!] \cap \nabla\sigma} \Psi^{\sigma}_{\Pi}(n)\ .
\end{aligned}$$

□

Proof of rule $(\Box_*)_{[p15]}$.. Assume that σ is stable.

$$
\begin{aligned}
&\langle \Pi \fatsemi \sigma \Vdash^{\mu} \Box\, \varphi \rangle \\
&\quad \iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \Box\, \varphi \\
&\quad \iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \forall i \in \operatorname{dom} w,\ (w, i) \models^{\mathbf{w}} \varphi \\
&\quad \iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \forall i \in \operatorname{dom} w,\ w^i \models^{\mathbf{w}} \varphi \\
&\quad \iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \forall i \in \mathbb{N}_1,\ i \in \operatorname{dom} w \Rightarrow w^i \models^{\mathbf{w}} \varphi \\
&\quad \iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ \forall i \in \mathbb{N}_1,\ \#w \geqslant i \Rightarrow w^i \models^{\mathbf{w}} \varphi \\
&\quad \iff \forall x \in \left\{ w^i \;\middle|\; i \in \mathbb{N}_1, w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!), \#w \geqslant i \right\},\ x \models^{\mathbf{w}} \varphi \\
&\quad \iff \forall x \in \left\{ w^{n+1} \;\middle|\; n \in \mathbb{N}, w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!), \#w \geqslant n+1 \right\},\ x \models^{\mathbf{w}} \varphi \\
&\quad \iff \forall x \in \left\{ w^{n+1} \;\middle|\; n \in \mathbb{N}, w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!), \#w \geqslant n \right\} \setminus \{\lambda\},\ x \models^{\mathbf{w}} \varphi \\
&\quad \iff \forall x \in {}^{\mathcal{R}}(\!|\sigma[\omega]^* (\Pi) \fatsemi \sigma|\!) \setminus \{\lambda\},\ x \models^{\mathbf{w}} \varphi \\
&\quad \iff \forall x \in {}^{\mathcal{R}}(\!|\sigma[\omega]^* (\Pi) \fatsemi \star\sigma|\!),\ x \models^{\mathbf{w}} \varphi \\
&\quad \iff \langle \sigma[\omega]^* (\Pi) \fatsemi \star\sigma \Vdash^{\mathbf{w}} \varphi \rangle\ .
\end{aligned}
$$

□

Proof of rule $(\Box_{\hbar})_{[p15]}$. Using Lemma 1[p5] and Remark 10[p14]. Assume that σ is unstable but can be stabilised, with $\hbar\sigma \in \mathbb{N}_1$.

$$
\begin{aligned}
\langle \Pi \fatsemi \sigma \Vdash^{\mu} \Box\, \varphi \rangle &\iff \left\langle \Pi \fatsemi \sigma \Vdash^{\mu} \left[\bigwedge_{k=0}^{\hbar\sigma-1} \circ^k \varphi \right] \wedge \circ^{\hbar\sigma} \Box\, \varphi \right\rangle \\
&\iff \underbrace{\left\langle \Pi \fatsemi \sigma \Vdash^{\mu} \bigwedge_{k=0}^{\hbar\sigma-1} \circ^k \varphi \right\rangle}_{A} \wedge \left\langle \Pi \fatsemi \sigma \Vdash^{\mu} \circ^{\hbar\sigma} \Box\, \varphi \right\rangle \\
&\iff A \wedge \left\langle \Pi^{\hbar\sigma}_{\sigma} \fatsemi \sigma \blacktriangleleft \hbar\sigma \Vdash^{\mu} \Box\, \varphi \right\rangle \\
&\iff A \wedge \left\langle \Pi^{\hbar\sigma}_{\sigma} \fatsemi \star(\sigma \triangleleft \hbar\sigma) \Vdash^{\mu} \Box\, \varphi \right\rangle \\
&\iff \left\langle \Pi \fatsemi \sigma \Vdash^{\mu} \bigwedge_{k=0}^{\hbar\sigma-1} \circ^k \varphi \right\rangle \wedge \left\langle \Pi^{\hbar\sigma}_{\sigma} \fatsemi \sigma \triangleleft \hbar\sigma \Vdash^{\mu} \Box\, \varphi \right\rangle\ .
\end{aligned}
$$

□

Proof of rule $(\neg X)_{[p15]}$.

$$
\langle \Pi \fatsemi \sigma \Vdash^{\mu} \neg X \rangle \iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mu} \neg X
$$

$$
\begin{aligned}
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ 1 \notin \operatorname{dom} w \vee w(1) \notin X \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ 1 \notin \operatorname{dom} w \vee w(1) \in \mathcal{R} \setminus X \\
&\iff \forall w \in {}^{\mathcal{R}}(\!|\Pi \fatsemi \sigma|\!),\ w \models^{\mathbf{w}} \mathcal{R} \setminus X \\
&\iff \langle \Pi \fatsemi \sigma \ \Vdash^{\mathbf{w}} \ \mathcal{R} \setminus X \rangle \ .
\end{aligned}
$$

□