H-0223 (H0405-001) May 2, 2004
Computer Science

IBM Research Report

Basic Results on the Semantics of Accellera PSL 1.1 Foundation Language

John Havlicek[1], Dana Fisman[2,3], Cindy Eisner[2]

[1]Motorola, Inc.

[2]IBM Research Division
Haifa Research Laboratory
Mt. Carmel 31905
Haifa, Israel

[3]Weizmann Institute of Science

Research Division
Almaden - Austin - Beijing - Haifa - India - T. J. Watson - Tokyo - Zurich

Basic Results on the Semantics of Accellera PSL 1.1 Foundation Language

John Havlicek[1] Dana Fisman[2,3] Cindy Eisner[2]

[1] Motorola, Inc.
[2] IBM Haifa Research Lab
[3] Weizmann Institute of Science

Abstract A number of technical consequences of the formal definitions of the semantics of Accellera PSL 1.1 Foundation Language are proved. These include direct characterizations of the semantics of derived LTL operators, duality of until operators, and the semantic correspondences that underly the clock rewrite rules given in Appendix B of the Accellera PSL 1.1 Language Reference Manual. The Prefix/Extension Theorem of [4] is shown to hold for PSL 1.1 Foundation Language. Results concerning the weak and strong promotions of boolean expressions and of Sequential Extended Regular Expressions to formulas are also proved. This work has supported the analysis and review of the formal semantics of PSL 1.1 Foundation Language and the effort to achieve semantic alignment between Accellera SystemVerilog 3.1 Assertions and PSL 1.1 Foundation Language.

Contents

1 Introduction

Accellera Property Specification Language 1.1 [1], abbreviated as *PSL 1.1*, is a standard language for precisely defining temporal properties of designs. The language is broadly divided into the *Foundation Language* and the *Optional Branching Extension*. This report is concerned only with the Foundation Language and does not discuss further the Optional Branching Extension. The Foundation Language is a linear temporal logic that includes:

- Standard boolean operators on formulas (negation, conjunction, disjunction).
- Standard LTL operators (globally, eventually, strong and weak nexttime, strong and weak until).
- A clocking operator for defining the granularity of time, which may differ from one part of a formula to another.
- *Sequential Extended Regular Expressions*, or (SEREs), for defining finite-length regular patterns, together with strong and weak promotions of SEREs to formulas and an implication operator for predicating a formula on match of the pattern specified by a SERE.
- An operator for aborting a formula "asynchronously" on satisfaction of a boolean condition.
- Numerous derived operators that abbreviate the writing of useful combinations of more basic operators.

The Foundation Language is defined with respect to boolean expressions over a given set of atomic propositions. The boolean expressions are the building blocks for the SEREs. The Foundation Language also provides both strong and weak promotions of boolean expressions to formulas of the logic, in analogy with the strong/weak pairings of the LTL operators and the strong/weak promotions of SEREs. As a result the clocking operator of the logic is strengthless, as in [5].

The formal syntax and semantics of the Foundation Language is defined in Appendix B of [1]. Appendix B gives separate explicit definitions for the syntax and semantics of *unclocked* and *clocked* SEREs and formulas.[1] The unclocked SEREs and formulas involve no clocking operator, and their semantics is defined with respect to a path. The clocked SEREs and formulas can involve instances of the clocking operator, and their semantics is defined with respect to a path and a clock context. Intuitively, an instance of the clocking operator coarsens the granularity of time so that, for instance, the nexttime operator moves not to the next state on the path, but rather to the next state where the clock "ticks". In both cases, the definitions are given explicitly only for generating sets of basic SERE and formula operators.

The purpose of this report is to prove a number of technical consequences of the formal definitions in Appendix B. One use of these results has been as "sanity checks" on the quality of the formal definitions. Since the formal definitions are

[1] As shown in Section 5 below, the semantics of clocked SEREs and formulas can be derived from the semantics of unclocked SEREs and formulas using the rewrite rules. Appendix B gives the explicit definitions of the clocked semantics for didactic reasons.

terse and given explicitly only for the basic operators, some effort is involved in the analysis of semantic relationships, especially those involving derived operators. Another use of the results has been in the alignment effort between Accellera SystemVerilog 3.1 Assertions [2] (abbreviated as *SVA 3.1*) and PSL 1.1 Foundation Language. One of the primary goals of that effort was to provide a mapping from from a subset of SVA 3.1 Concurrent Assertions to PSL 1.1 Foundation Language and to prove semantic equivalence of an SVA 3.1 assertion from the subset and its image under the mapping. In the course of that work, a number of technical lemmas about PSL 1.1 Foundation Language were proved, and most of them are collected in this report. Finally, in several cases the work leading to the present results uncovered flaws in the formal semantics of SVA 3.1 and/or draft definitions of the formal semantics of PSL 1.1 Foundation Language. Known errors have been corrected in SVA 3.1a and the final version of PSL 1.1 Foundation Language. Thus, the work leading to the results presented in this report has improved the quality of both Accellera languages.

The technical results in this report are not mathematically deep. They are, for the most part, intuitive but not entirely obvious. As a result, this report should be accessible to a reader who is familiar with elementary set theory and functions and who is comfortable reading Appendix B of [1]. Some of the results in this report have been proved independently by mechanical means [6].

The rest of this report is organized as follows.

- Section 2 gives preliminaries and notations and introduces the extended alphabet used in definition of the semantics in Appendix B of [1].
- Section 3 discusses the way the primitive forms for this report differ from those in Appendix B.
- Section 4 provides direct semantics of the derived LTL operators over proper words. Duality of until operators is also discussed.
- Section 5 presents the rewrite rules from Appendix B for transforming clocked SEREs and formulas into unclocked versions. For both SEREs and formulas, the semantic correspondence between a clocked entity and the rewritten unclocked entity is proved.
- Section 6 contains a few results on clock ticks.
- Section 7 presents results on the semantics of tight satisfaction (i.e., matching) of SEREs.
- Section 8 discusses promotion of SEREs to formulas. Most of the unclocked results have been presented in the context of a simpler logic in [3].
- Section 9 proves that the Prefix/Extension Theorem of [4] holds for PSL 1.1 Foundation Language, both in unclocked and clocked forms.
- Section 10 discusses the promotion of boolean expressions to formulas and their relation to SERE formulas.
- Section 11 shows that inductive definitions of the unclocked and clocked PSL formula satisfaction relations can be given for the set of proper words without relying on the definitions of formula satisfaction for non-proper words.

- Section 12 presents some miscellaneous lemmas on formulas, primarily from the work on mapping from SVA 3.1 to PSL 1.1.

For reference, the semantic definitions from Appendix B of [1] are copied in an appendix with notations adapted to the conventions of this report.

2 Preliminaries and notation

Throughout the rest of this report, "PSL" is used to mean "PSL 1.1 Foundation Language". For concreteness, this report uses the Verilog flavor of PSL and sets language terminals using a typewriter font. Braces are used around operands of certain SERE operators and around SEREs that are promoted to formulas. Many of these braces were required in earlier versions of the language but are optional in [1]. The letters i, j, and k always denote non-negative integers.

Let $\mathbf{P}$ denote the underlying set of atomic propositions. The ordinary alphabet for the semantics of PSL is the power set $2^{\mathbf{P}}$. Let $\mathcal{B}$ denote the set of boolean expressions. There is understood to be a relation of boolean satisfaction $\models \subseteq 2^{\mathbf{P}} \times \mathcal{B}$. The notation "$\ell \models b$" (respectively, "$\ell \not\models b$") means that $(\ell, b) \in \models$ (respectively, $(\ell, b) \notin \models$). For $\ell \in 2^{\mathbf{P}}$ and $b, c \in \mathcal{B}$, it is understood that $\ell \models b$ iff $\ell \not\models \texttt{!}b$ and that $\ell \models b \texttt{ \&\& } c$ iff both $\ell \models b$ and $\ell \models c$. The "true" (respectively, "false") element of $\mathcal{B}$ is denoted "TRUE" (respectively, "FALSE"), and it is understood that

$$\ell \models \text{TRUE} \quad \text{and} \quad \ell \not\models \text{FALSE}$$

for all $\ell \in 2^{\mathbf{P}}$.

The extended alphabet for the semantics of PSL is

$$\Sigma = 2^{\mathbf{P}} \cup \{\top, \bot\}$$

The relation $\models$ is extended to letters in Σ by defining

$$\top \models b \quad \text{and} \quad \bot \not\models b$$

for all $b \in \mathcal{B}$. Unlike letters of the ordinary alphabet, $\top \models$ FALSE and $\bot \not\models$ TRUE. Let $\overline{\top} = \bot$, $\overline{\bot} = \top$, and $\overline{\ell} = \ell$ for $\ell \in 2^{\mathbf{P}}$.

A *word* over Σ is a sequence of letters from Σ. The concatenation of word v followed by word w is denoted vw. If v is infinite, then $vw = v$. Word u is a *prefix* of word w, denoted $u \preceq w$, iff there exists a word v such that $w = uv$. Word w is an *extension* of word u, denoted $w \succeq u$, iff u is a prefix of w. Word v is a *suffix* of word w iff there exists a finite word u such that $w = uv$.

The number of letters in word w is called the *length* of w and is denoted $|w|$. If w is infinite, then $|w|$ is ω. The letters of a word are assumed to be indexed consecutively beginning at zero. If $|w| = 0$, then w has no letters and is said to be *empty*. If $|w| > 0$, then the first letter of w is denoted w^0; if $|w| > 1$, then the second letter of w is denoted w^1; and so forth. Let $\bar{w}$ denote the word over Σ such that $\bar{w}^i = \overline{w^i}$. In other words, $\bar{w}$ is obtained from w by interchanging $\top$ with $\bot$.

If $i < |w|$, then $w^{i\cdot\cdot}$ denotes the suffix of w beginning at w^i. In other words, $w^{i\cdot\cdot} = w^i w^{i+1} \cdots w^{|w|-1}$ if w is finite, and $w^{i\cdot\cdot} = w^i w^{i+1} \cdots$ if w is infinite. If $i \geq |w|$, then $w^{i\cdot\cdot}$ denotes the empty word. If $i \leq j < |w|$, then $w^{i..j}$ denotes the finite subword $w^i \cdots w^j$ of w. If $h < i < |w|$, perhaps $h < 0$, then $w^{i..h}$ denotes the empty word. ℓ^k denotes the finite word of length k each letter of which is ℓ. ℓ^ω denotes the infinite word each letter of which is ℓ.

The semantics of matching the patterns of SEREs is defined via a relation of *tight satisfaction* by finite (possibly empty) words. In the unclocked case, the relation

is binary and defines when a finite word w tightly satisfies an unclocked SERE r, denoted

$$w \models\!\!\models r$$

In the clocked case, the relation is ternary and defines when a finite word w tightly satisfies a SERE r in the context of the clock represented by boolean expression c, denoted

$$w \models\!\!\models^c r$$

The semantics of PSL formulas is defined via a relation of *satisfaction* by finite (possibly empty) or infinite words. In the unclocked case, the relation is binary and defines when a word w satisfies an unclocked formula f, denoted

$$w \models f$$

In the clocked case, the relation is ternary and defines when a word w satisfies a formula f in the context of the clock represented by boolean expression c, denoted

$$w \models^c f$$

The two preceding satisfaction relations are also called unclocked and clocked *neutral satisfaction* (respectively) to distinguish them from the following unclocked and clocked *weak* $(-)$ and *strong* $(+)$ satisfaction relations. For w a word over Σ and f an unclocked PSL formula,

$$\begin{array}{lll} w \models^- f & \text{iff} & w\top^\omega \models f \\ w \models^+ f & \text{iff} & w\bot^\omega \models f \end{array}$$

For w a word over Σ, c a boolean expression, and f a PSL formula,

$$\begin{array}{lll} w \models^{c-} f & \text{iff} & w\top^\omega \models^c f \\ w \models^{c+} f & \text{iff} & w\bot^\omega \models^c f \end{array}$$

3 Primitives

Many of the results in this report are proved by induction over SERE or formula structure. The primitive SERE and formula operators for these proofs differ slightly from those presented in Appendix B of [1]. This section describes the differences.

In Appendix B of [1], "`[*0]`" is a primitive SERE, and "`[*]`" is the primitive repetition operator for SEREs. In this report, we prefer to use "`[+]`" as the primitive repetition operator for proofs by induction over SERE structure because the arguments for "`[+]`" tend to require less case splitting than for "`[*]`". This is because "r`[*]`" intuitively means "zero or more repetitions of r". In an inductive proof, the argument for "zero repetitions" is typically redundant with the argument for "`[*0]`" and usually must be handled separately from the argument for "one or more repetitions". On the other hand,

$$r\texttt{[+]} \stackrel{\text{def}}{=} r\ \texttt{;}\ r\texttt{[*]}$$

which intuitively means "one or more repetitions of r". This change of primitives for the proofs is justified by Lemmas 3.3 and 3.4 below.

The following two lemmas give direct semantics for r`[+]` in the unclocked and the clocked cases.

Lemma 3.1. *Let w be a finite word over Σ, and let r be an unclocked* SERE*. Then $w \models r$`[+]` *iff there exist $k > 0$ and $w_1, \ldots, w_k$ such that $w = w_1 \cdots w_k$ and $w_j \models r$ for each $1 \leq j \leq k$.*

Proof.

$w \models r$`[+]`
iff $w \models r\ \texttt{;}\ r\texttt{[*]}$
iff there exist w_1, u_1 such that $w = w_1 u_1$ and $w_1 \models r$ and $u_1 \models r$`[*]`

By definition,

$u_1 \models r$`[*]`
iff $u_1 \models$ `[*0]` or there exist w_2, u_2 such that $|w_2| > 0$ and $u_1 = w_2 u_2$ and $w_2 \models r$ and $u_2 \models r$`[*]`
iff $|u_1| = 0$ or there exist w_2, u_2 such that $|w_2| > 0$ and $u_1 = w_2 u_2$ and $w_2 \models r$ and $u_2 \models r$`[*]`

By repeating the application of this definition to the suffix u_j and using the fact that $|w|$ bounds the number of times the suffix can be split, it follows that

$u_1 \models r$`[*]`
iff $|u_1| = 0$ or there exist $k \geq 2$ and non-empty $w_2, \ldots, w_k$ such that $u_1 = w_2 \cdots w_k$ and $w_j \models r$ for each $2 \leq j \leq k$

Therefore

$w \models r$`[+]`
iff
(A):
there exist w_1, u_1 such that $w = w_1 u_1$ and $w_1 \models r$ and either $|u_1| = 0$ or there exist $k \geq 2$ and non-empty $w_2, \ldots, w_k$ such that $u_1 = w_2 \cdots w_k$ and $w_j \models r$ for each $2 \leq j \leq k$

Let

(B):
there exist $k > 0$ and $w_1, \ldots, w_k$ such that $w = w_1 \cdots w_k$ and $w_j \models r$ for each $1 \leq j \leq k$

Assume (A). If $|u_1| \neq 0$, then (B) clearly follows. Otherwise, (B) follows by letting $k = 1$.

Assume (B). Suppose w is empty. Then all of the w_j are empty, and, since $k > 0$, $w = w_1 \models r$. In this case, (A) holds with $k = 1$ and $u_1 = 0$. Otherwise, w is non-empty, so there is at least one non-emtpy w_j. Discard all the empty w_j and reindex. Then (A) holds, either with $k = 1$ and $|u_1| = 0$ or with $k \geq 2$. □

Lemma 3.2. *Let w be a finite word over Σ, let c be a boolean expression, and let r be a* SERE*. Then $w \models^c r$`[+]` iff there exist $k > 0$ and $w_1, \ldots, w_k$ such that $w = w_1 \cdots w_k$ and $w_j \models^c r$ for each $1 \leq j \leq k$.*

Proof. Analogous to the proof of Lemma 3.1. □

The following two lemmas give the semantics of r`[*]` as derived from `[*0]` and r`[+]`.

Lemma 3.3. *Let w be a finite word over Σ, and let r be an unclocked* SERE*. Then $w \models r$`[*]` iff $w \models$ `{[*0]} || {`r`[+]}`.*

Proof.

$w \models r$`[*]`
iff either
  $w \models$ `[*0]`
  or
  there exist u, v such that $|u| > 0$ and $w = uv$ and $u \models r$ and $v \models r$`[*]`
iff [for ($\Leftarrow$), if $|u| = 0$, then $w = v \models r$`[*]`]
  either
  $w \models$ `[*0]`
  or
  there exist u, v such that $w = uv$ and $u \models r$ and $v \models r$`[*]`
iff either
  $w \models$ `[*0]`
  or
  $w \models r$ `;` r`[*]`
iff either
  $w \models$ `[*0]`
  or
  $w \models r$`[+]`
iff $w \models$ `{[*0]} || {`r`[+]}`

□

Lemma 3.4. *Let w be a finite word over Σ, let c be a boolean expression, and let r be a* SERE. *Then $w \models^c r\texttt{[*]}$ iff $w \models^c \texttt{\{[*0]\} || \{}r\texttt{[+]\}}$.*

Proof. Analogous to the proof of Lemma 3.3. □

Appendix B of [1] lists both the strong and weak boolean formulas among the primitive formula types. Given formula and boolean negation, though, only one of the boolean formula forms need be a primitive. In the proofs in this report, we regard only the strong boolean formula form as a primitive. The next lemmas justify this simplification.

Lemma 3.5 (Duality of Boolean Satisfaction). *Let $\ell \in \Sigma$, and let b be a boolean expression. Then $\ell \Vdash b$ iff $\bar{\ell} \not\Vdash \texttt{!}b$.*

Proof. If $\ell \in 2^{\mathbf{P}}$, then $\ell = \bar{\ell}$ and the result follows because the relation $\Vdash$ has the property that $\ell \Vdash b$ iff $\ell \not\Vdash \texttt{!}b$ when $\ell \in 2^{\mathbf{P}}$. If $\ell = \top$, then $\ell \Vdash b$ and $\bar{\ell} = \bot \not\Vdash \texttt{!}b$. If $\ell = \bot$, then $\ell \not\Vdash b$ and $\bar{\ell} = \top \Vdash \texttt{!}b$. □

The following notation is used to eliminate ambiguity between boolean expression negation and boolean formula negation.

Notation 3.6. *Let b be a boolean expression.*

- $\mathsf{s}(b)$ *denotes the strong boolean formula* $b\texttt{!}$.
- $\mathsf{w}(b)$ *denotes the weak boolean formula* b.

□

Lemma 3.7 (Unclocked Duality of Boolean Formulas). *Let b be a boolean expression, and let w be a word over Σ. Then*

1. $w \models \mathsf{w}(b)$ *iff* $w \models \texttt{!}\mathsf{s}(\texttt{!}b)$
2. $w \models \mathsf{s}(b)$ *iff* $w \models \texttt{!}\mathsf{w}(\texttt{!}b)$

Proof. Note that 2 follows from 1 by negating both the boolean expression and the formulas. Here is the proof of 1:

$w \models \texttt{!}\mathsf{s}(\texttt{!}b)$
iff $\bar{w} \not\models \mathsf{s}(\texttt{!}b)$
iff $\neg(|\bar{w}| > 0$ and $\bar{w}^0 \Vdash \texttt{!}b)$
iff $|\bar{w}| = 0$ or $\bar{w}^0 \not\Vdash \texttt{!}b$
iff [Lemma 3.5; $|\bar{w}| = |w|$]
$|w| = 0$ or $w^0 \Vdash b$
iff $w \models \mathsf{w}(b)$

□

Lemma 3.8 (Clocked Duality of Boolean Formulas). *Let b, c be boolean expressions, and let w be a word over Σ. Then*

1. $w \models^c \mathsf{w}(b)$ *iff* $w \models^c \mathsf{!s}(\mathsf{!}b)$

2. $w \models^c \mathsf{s}(b)$ *iff* $w \models^c \mathsf{!w}(\mathsf{!}b)$

Proof. Note that 2 follows from 1 by negating both the boolean expression and the formulas. Here is the proof of 1:

$w \models^c \mathsf{!s}(\mathsf{!}b)$
iff $\bar{w} \not\models^c \mathsf{s}(\mathsf{!}b)$
iff $\neg$(there exists $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of c and $\bar{w}^j \not\models \mathsf{!}b$)
iff for all $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of c, $\bar{w}^j \not\models \mathsf{!}b$
iff [Lemma 3.5]
for all $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of c, $w^j \not\models b$
iff $w \models^c \mathsf{w}(b)$

□

4 Direct semantics of LTL operators

This section gives direct unclocked and clocked semantics of the derived LTL operators `X` (weak nexttime), `F` (eventually), `G` (globally), and `W` (weak until). There are some nuances to the semantics for general words over the extended alphabet Σ. However, the words over Σ that are of primary interest are those that are *proper* according to the following definition.

Definition 4.1. *A word w over Σ is called* proper *if it is of the form $w = uv$, where u is a word over $2^{\mathbf{P}}$ and either v is empty or $v = \top^\omega$ or $v = \bot^\omega$.*

The set of proper words includes all the words over $2^{\mathbf{P}}$ and all the words over Σ that are required for recursive evaluation of unclocked and clocked formula satisfaction by proper words. This fact is explained further in Section 11.

The results of this section show that the unclocked semantics of the LTL operators over proper words are the usual ones. In particular, duality between weak and strong untils is proved for proper words in the usual way. The clocked semantics of the LTL operators over proper words are intuitively similar, but there is a subtlety in one of the duality relationship for untils.

Lemma 4.2 (Direct Unclocked Semantics of `X`). *Let f be an unclocked PSL formula, and let w be a word over Σ. Then $w \models \mathtt{X}\ f$ iff either $|w| \leq 1$ or $w^{1..} \models f$*

Proof.

$w \models \mathtt{X}\ f$
iff $w \models \mathtt{!X!}\ !f$
iff $\bar{w} \not\models \mathtt{X!}\ !f$
iff $\neg(|w| > 1$ and $\bar{w}^{1..} \models \mathtt{!}\ f)$
iff either $|w| \leq 1$ or $w^{1..} \models f$

□

Lemma 4.3 (Direct Clocked Semantics of `X`). *Let f be an PSL formula, let c be a boolean expression, and let w be a word over Σ. Then $w \models^c \mathtt{X}\ f$ iff for all $0 \leq j < k < |w|$ such that $\bar{w}^{0..j}$ and $\bar{w}^{j+1..k}$ are clock ticks of c, $w^{k..} \models^c f$*

Proof.

$w \models^c \mathtt{X}\ f$
iff $w \models^c \mathtt{!X!}\ !f$
iff $\bar{w} \not\models^c \mathtt{X!}\ !f$
iff $\neg$(there exist $0 \leq j < k < |w|$ such that $\bar{w}^{0..j}$ and $\bar{w}^{j+1..k}$ are clock ticks of c and $\bar{w}^{k..} \models^c \mathtt{!}\ f)$
iff for all $0 \leq j < k < |w|$ such that $\bar{w}^{0..j}$ and $\bar{w}^{j+1..k}$ are clock ticks of c, $w^{k..} \models^c f$

□

Lemma 4.4 (Direct Unclocked Semantics of F). *Let f be an unclocked PSL formula, and let w be a proper word over Σ. Then $w \models \mathtt{F}\ f$ iff there exists $0 \leq k < |w|$ such that $w^{k\cdot\cdot} \models f$.*

Proof.

$w \models \mathtt{F}\ f$
iff $w \models [\text{TRUE}\ \mathtt{U}\ f]$
iff there exists $0 \leq k < |w|$ such that $w^{k\cdot\cdot} \models f$ and for all $0 \leq j < k$, $w^{j\cdot\cdot} \models \text{TRUE}$
iff (A):
there exists $0 \leq k < |w|$ such that $w^{k\cdot\cdot} \models f$ and for all $0 \leq j < k$, $w^j \neq \bot$

Let

(B):
there exists $0 \leq k < |w|$ such that $w^{k\cdot\cdot} \models f$

Clearly, (A) implies (B). Assume (B). If $w^k \neq \bot$, then, since w is proper, $w^j \neq \bot$ for all $0 \leq j < k$, and so (A) holds. Otherwise, $w^k = \bot$. Let k' be the minimal index such that $w^{k'} = \bot$. Then, since w is proper, $w^{k'\cdot\cdot} = \bot^\omega = w^{k\cdot\cdot} \models f$, and for all $0 \leq j < k'$, $w^j \neq \bot$. Therefore (A) holds. □

Lemma 4.5 (Direct Clocked Semantics of F). *Let f be a PSL formula, let c be a boolean expression, and let w be a proper word over Σ. Then $w \models^c \mathtt{F}\ f$ iff there exists $k < |w|$ such that $w^k \models c$ and $w^{k\cdot\cdot} \models^c f$.*

Proof.

$w \models^c \mathtt{F}\ f$
iff $w \models^c [\text{TRUE}\ \mathtt{U}\ f]$
iff there exists $k < |w|$ such that $w^k \models c$ and $w^{k\cdot\cdot} \models^c f$ and for all $0 \leq i < k$ such that $\bar{w}^i \models c$, $w^{i\cdot\cdot} \models^c \text{TRUE}$
iff there exists $k < |w|$ such that $w^k \models c$ and $w^{k\cdot\cdot} \models^c f$ and for all $0 \leq i < k$, if $\bar{w}^i \models c$ then for all $i \leq j < |w|$, if $\bar{w}^{i\cdot\cdot j}$ is a clock tick of c then $w^j \models \text{TRUE}$
iff (A):
there exists $k < |w|$ such that $w^k \models c$ and $w^{k\cdot\cdot} \models^c f$ and for all $0 \leq i < k$, if $\bar{w}^i \models c$ then for all $i \leq j < |w|$, if $\bar{w}^{i\cdot\cdot j}$ is a clock tick of c then $w^j \neq \bot$

Let

(B):
there exists $k < |w|$ such that $w^k \models c$ and $w^{k\cdot\cdot} \models^c f$

Clearly, (A) implies (B). Assume (B). Since $w^k \models c$, $w^k \neq \bot$. Since w is proper, $w^j \neq \bot$ for all $0 \leq j \leq k$. Suppose that $0 \leq i < k$ and $\bar{w}^i \models c$ and $i \leq j < |w|$ and $\bar{w}^{i\cdot\cdot j}$ is a clock tick of c. Suppose $i < j$. Then $\bar{w}^i \models !c$. Since $\bar{w}^i \models c$, it follows that $\bar{w}^i = \top$, hence $w^i = \bot$, a contradiction. Therefore $j = i < k$, and so $w^j \neq \bot$. This proves (A). □

Lemma 4.6 (Direct Unclocked Semantics of G). *Let f be an unclocked PSL formula, and let w be a proper word over Σ. Then $w \models \mathtt{G}\ f$ iff for all $0 \leq k < |w|$, $w^{k\cdot\cdot} \models f$.*

Proof.

$w \models \mathtt{G}\ f$
iff $w \models \mathtt{![TRUE\ U\ !}f\mathtt{]}$
iff $\neg(\bar{w} \models \mathtt{[TRUE\ U\ !}f\mathtt{]})$
iff [Lemma 4.4]
$\neg$(there exists $0 \leq k < |w|$ such that $\bar{w}^{k\cdot\cdot} \models \mathtt{!}f$)
iff for all $0 \leq k < |w|$, $\bar{w}^{k\cdot\cdot} \not\models \mathtt{!}f$
iff for all $0 \leq k < |w|$, $w^{k\cdot\cdot} \models f$

□

Lemma 4.7 (Direct Clocked Semantics of G). *Let f be a PSL formula, let c be a boolean expression, and let w be a proper word over Σ. Then $w \models^c \mathtt{G}\ f$ iff for all $0 \leq k < |w|$ such that $\bar{w}^k \models c$, $w^{k\cdot\cdot} \models^c f$.*

Proof.

$w \models^c \mathtt{G}\ f$
iff $w \models^c \mathtt{![TRUE\ U\ !}f\mathtt{]}$
iff $\neg(\bar{w} \models^c \mathtt{[TRUE\ U\ !}f\mathtt{]})$
iff [Lemma 4.5]
$\neg$(there exists $0 \leq k < |w|$ such that $\bar{w}^k \models c$ and $\bar{w}^{k\cdot\cdot} \models^c \mathtt{!}f$)
iff for all $0 \leq k < |w|$ such that $\bar{w}^k \models c$, $\bar{w}^{k\cdot\cdot} \not\models^c \mathtt{!}f$
iff for all $0 \leq k < |w|$ such that $\bar{w}^k \models c$, $w^{k\cdot\cdot} \models^c f$

□

Lemma 4.8 (Direct Unclocked Semantics of W). *Let f, g be unclocked PSL formulas, and let w be a proper word over Σ. Then $w \models \mathtt{[}f\ \mathtt{W}\ g\mathtt{]}$ iff for all $0 \leq k < |w|$ such that $w^{k\cdot\cdot} \not\models f$, there exists $0 \leq j \leq k$ such that $w^{j\cdot\cdot} \models g$.*

Proof.

$w \models \mathtt{[}f\ \mathtt{W}\ g\mathtt{]}$
iff $w \models \mathtt{[}f\ \mathtt{U}\ g\mathtt{]}\ \mathtt{||}\ \mathtt{G}\ f$
iff either
$w \models \mathtt{[}f\ \mathtt{U}\ g\mathtt{]}$
or
$w \models \mathtt{G}\ f$
iff [Lemma 4.6]
(A):
either
1. there exists $0 \leq k < |w|$ such that $w^{k\cdot\cdot} \models g$ and for all $0 \leq j < k$, $w^{j\cdot\cdot} \models f$
or
2. for all $0 \leq k < |w|$, $w^{k\cdot\cdot} \models f$

Let

(B):
for all $0 \leq k < |w|$ such that $w^{k\cdot\cdot} \not\models f$, there exists $0 \leq j \leq k$ such that $w^{j\cdot\cdot} \models g$

Assume (A). Let $0 \leq k < |w|$ be such that $w^{k\cdot\cdot} \not\models f$. Then the first disjunct of (A) must hold, so there exists $0 \leq k' < |w|$ such that $w^{k'\cdot\cdot} \models g$ and for all $0 \leq j' < k'$, $w^{j'\cdot\cdot} \models f$. Therefore, $k' \leq k$, and so with $j = k'$ the conclusion of (B) holds. This proves (B).

Now assume (B). Suppose the second disjunct of (A) fails, so there exists $0 \leq k' < |w|$ such that $w^{k'\cdot\cdot} \not\models f$. Without loss of generality, k' is minimal. Therefore, for all $0 \leq j < k'$, $w^{j\cdot\cdot} \models f$. By (B), there exists $0 \leq k \leq k'$ such that $w^{k\cdot\cdot} \models g$, and so the first disjunct of (A) holds. □

Lemma 4.9 (Direct Clocked Semantics of `W`). *Let f, g be PSL formulas, let c be a boolean expression, and let w be a proper word over Σ. Then $w \models^c$ `[f W g]` iff for all $0 \leq k < |w|$ such that $\bar{w}^k \Vdash c$ and $w^{k\cdot\cdot} \not\models^c f$, there exists $0 \leq j \leq k$ such that $w^j \Vdash c$ and $w^{j\cdot\cdot} \models^c g$.*

Proof.

$w \models^c$ `[`f `W` g`]`
iff $w \models^c$ `[`f `U` g`] || G` f
iff either
  $w \models^c$ `[`f `U` g`]`
or
  $w \models^c$ `G` f
iff [Lemma 4.7]
(A):
either
1. there exists $0 \leq k < |w|$ such that $w^k \Vdash c$ and $w^{k\cdot\cdot} \models^c g$ and for all $0 \leq j < k$ such that $\bar{w}^j \Vdash c$, $w^{j\cdot\cdot} \models^c f$

or
2. for all $0 \leq k < |w|$ such that $\bar{w}^k \Vdash c$, $w^{k\cdot\cdot} \models^c f$.

Let

(B):
for all $0 \leq k < |w|$ such that $\bar{w}^k \Vdash c$ and $w^{k\cdot\cdot} \not\models^c f$, there exists $0 \leq j \leq k$ such that $w^j \Vdash c$ and $w^{j\cdot\cdot} \models^c g$

Assume (A). Let $0 \leq k < |w|$ be such that $\bar{w}^k \Vdash c$ and $w^{k\cdot\cdot} \not\models^c f$. Then the second disjunct of (A) cannot hold, so there exists $0 \leq k' < |w|$ such that $w^{k'} \Vdash c$ and $w^{k'\cdot\cdot} \models^c g$ and for all $0 \leq j' < k'$ such that $\bar{w}^{j'} \Vdash c$, $w^{j'\cdot\cdot} \models^c f$. Therefore, $k' \leq k$, and so with $j = k'$ the conclusion of (B) holds. This proves (B).

Now assume (B). Suppose the second disjunct of (A) fails, so there exists $0 \leq k' < |w|$ such that $\bar{w}^{k'} \Vdash c$ and $w^{k'\cdot\cdot} \not\models^c f$. Without loss of generality, k' is minimal. Therefore, for all $0 \leq j < k'$ such that $\bar{w}^j \Vdash c$, $w^{j\cdot\cdot} \models^c f$. By (B), there exists $0 \leq k \leq k'$ such that $w^k \Vdash c$ and $w^{k\cdot\cdot} \models^c g$, and so the first disjunct of (A) holds. This proves (A). □

Lemma 4.10 (Unclocked Duality of Untils). *Let f, g be unclocked PSL formulas, and let w be a proper word over Σ. Then*

1. $w \models \texttt{[}f\ \texttt{U}\ g\texttt{]}$ iff $w \models \texttt{![!}g\ \texttt{W (!}f\ \texttt{\&\& !}g\texttt{)]}$.

2. $w \models \texttt{[}f\ \texttt{W}\ g\texttt{]}$ iff $w \models \texttt{![!}g\ \texttt{U (!}f\ \texttt{\&\& !}g\texttt{)]}$.

Proof.

1. $w \models \texttt{![!}g\ \texttt{W (!}f\ \texttt{\&\& !}g\texttt{)]}$
   iff $\bar{w} \not\models \texttt{[!}g\ \texttt{W (!}f\ \texttt{\&\& !}g\texttt{)]}$
   iff [Lemma 4.8]
   ¬(for all $0 \leq k < |w|$ such that $\bar{w}^{k\cdot\cdot} \not\models \texttt{!}g$, there exists $0 \leq j \leq k$ such that $\bar{w}^{j\cdot\cdot} \models \texttt{!}f\ \texttt{\&\& !}g$)
   iff there exists $0 \leq k < |w|$ such that $w^{k\cdot\cdot} \models g$ and for all $0 \leq j \leq k$, $w^{j\cdot\cdot} \models f\ \texttt{||}\ g$
   iff [let k be minimal such that $w^{k\cdot\cdot} \models g$]
   there exists $0 \leq k < |w|$ such that $w^{k\cdot\cdot} \models g$ and for all $0 \leq j < k$, $w^{j\cdot\cdot} \models f$
   iff $w \models \texttt{[}f\ \texttt{U}\ g\texttt{]}$

2. $w \models \texttt{![!}g\ \texttt{U (!}f\ \texttt{\&\& !}g\texttt{)]}$
   iff $\bar{w} \not\models \texttt{[!}g\ \texttt{U (!}f\ \texttt{\&\& !}g\texttt{)]}$
   iff ¬(there exists $0 \leq k < |w|$ such that $\bar{w}^{k\cdot\cdot} \models \texttt{!}f\ \texttt{\&\& !}g$ and for all $0 \leq j < k$, $\bar{w}^{j\cdot\cdot} \models \texttt{!}g$)
   iff for all $0 \leq k < |w|$ such that $\bar{w}^{k\cdot\cdot} \models \texttt{!}f\ \texttt{\&\& !}g$, there exists $0 \leq j < k$ such that $\bar{w}^{j\cdot\cdot} \not\models \texttt{!}g$
   iff for all $0 \leq k < |w|$ such that $w^{k\cdot\cdot} \not\models f\ \texttt{||}\ g$, there exists $0 \leq j < k$ such that $w^{j\cdot\cdot} \models g$
   iff for all $0 \leq k < |w|$ such that $w^{k\cdot\cdot} \not\models f$, there exists $0 \leq j \leq k$ such that $w^{j\cdot\cdot} \models g$
   iff [Lemma 4.8]
   $w \models \texttt{[}f\ \texttt{W}\ g\texttt{]}$

□

Lemma 4.11 (Clocked Approximate Duality of Untils). *Let f, g be PSL formulas, let c be a boolean expression, and let w be a proper word over Σ. Then*

1. $w \models^c \texttt{[}f\ \texttt{U}\ g\texttt{]}$ iff $w \models^c \texttt{![!}g\ \texttt{W (!}f\ \texttt{\&\& !}g\texttt{)]}$.

2. If $w \models^c \texttt{[}f\ \texttt{W}\ g\texttt{]}$, then $w \models^c \texttt{![!}g\ \texttt{U (!}f\ \texttt{\&\& !}g\texttt{)]}$. If $w \models^c \texttt{![!}g\ \texttt{U (!}f\ \texttt{\&\& !}g\texttt{)]}$ and $\bot^\omega \not\models^c g$, then $w \models^c \texttt{[}f\ \texttt{W}\ g\texttt{]}$.

Proof.

1. $w \models^c \texttt{![!}g\ \texttt{W (!}f\ \texttt{\&\& !}g\texttt{)]}$
   iff $\bar{w} \not\models^c \texttt{[!}g\ \texttt{W (!}f\ \texttt{\&\& !}g\texttt{)]}$
   iff [Lemma 4.9]
   ¬(for all $0 \leq k < |w|$ such that $w^k \models c$ and $\bar{w}^{k\cdot\cdot} \not\models^c \texttt{!}g$, there exists

$0 \leq j \leq k$ such that $\bar{w}^j \Vdash c$ and $\bar{w}^{j\cdot\cdot} \models^c \texttt{!}f \texttt{ \&\& !}g$)

iff (A):

there exists $0 \leq k < |w|$ such that $w^k \Vdash c$ and $w^{k\cdot\cdot} \models^c g$ and for all $0 \leq j \leq k$ such that $\bar{w}^j \Vdash c$, $w^{j\cdot\cdot} \models^c f \texttt{ || } g$

By definition,

$w \models^c \texttt{[}f \texttt{ U } g\texttt{]}$

iff (B):

there exists $0 \leq k < |w|$ such that $w^k \Vdash c$ and $w^{k\cdot\cdot} \models^c g$ and for all $0 \leq j < k$ such that $\bar{w}^j \Vdash c$, $w^{j\cdot\cdot} \models^c f$

Clearly (B) implies (A).

Assume (A). Take k to be minimal such that $w^k \Vdash c$ and $w^{k\cdot\cdot} \models^c g$. Let $0 \leq j < k$ be such that $\bar{w}^j \Vdash c$. By (A), $w^{j\cdot\cdot} \models^c f \texttt{ || } g$. If $w^j \not\Vdash c$, then $w^j = \bot$, and so, since w is proper, $w^k = \bot$, a contradiction. Therefore, $w^j \Vdash c$, and so by the minimality of k, $w^{j\cdot\cdot} \not\models^c g$. Therefore $w^{j\cdot\cdot} \models^c f$. This proves (B).

2. $w \models^c \texttt{![!}g \texttt{ U (!}f \texttt{ \&\& !}g\texttt{)]}$

iff $\bar{w} \not\models^c \texttt{[!}g \texttt{ U (!}f \texttt{ \&\& !}g\texttt{)]}$

iff $\neg$(there exists $0 \leq k < |w|$ such that $\bar{w}^k \Vdash c$ and $\bar{w}^{k\cdot\cdot} \models^c \texttt{!}f \texttt{ \&\& !}g$ and for all $0 \leq j < k$ such that $w^j \Vdash c$, $\bar{w}^{j\cdot\cdot} \models^c \texttt{!}g$)

iff for all $0 \leq k < |w|$ such that $\bar{w}^k \Vdash c$ and $\bar{w}^{k\cdot\cdot} \models^c \texttt{!}f \texttt{ \&\& !}g$, there exists $0 \leq j < k$ such that $w^j \Vdash c$ and $\bar{w}^{j\cdot\cdot} \not\models^c \texttt{!}g$

iff (A):

for all $0 \leq k < |w|$ such that $\bar{w}^k \Vdash c$ and $w^{k\cdot\cdot} \not\models^c f \texttt{ || } g$, there exists $0 \leq j < k$ such that $w^j \Vdash c$ and $w^{j\cdot\cdot} \models^c g$

By Lemma 4.9

$w \models^c \texttt{[}f \texttt{ W } g\texttt{]}$

iff (B):

for all $0 \leq k < |w|$ such that $\bar{w}^k \Vdash c$ and $w^{k\cdot\cdot} \not\models^c f$, there exists $0 \leq j \leq k$ such that $w^j \Vdash c$ and $w^{j\cdot\cdot} \models^c g$

Assume (B). Let $0 \leq k < |w|$ be such that $\bar{w}^k \Vdash c$ and $w^{k\cdot\cdot} \not\models^c f \texttt{ || } g$. Then $w^{k\cdot\cdot} \not\models^c f$ and $w^{k\cdot\cdot} \not\models^c g$. Then by (B), there exists $0 \leq j < k$ such that $w^j \Vdash c$ and $w^{j\cdot\cdot} \models^c g$. This proves (A).

Assume (A) and assume that $\bot^\omega \not\models^c g$. Let $0 \leq k < |w|$ be such that $\bar{w}^k \Vdash c$ and $w^{k\cdot\cdot} \not\models^c f$. If $w^{k\cdot\cdot} \not\models^c g$, then by (A), there exists $0 \leq j < k$ such that $w^j \Vdash c$ and $w^{j\cdot\cdot} \models g$, and so the conclusion of (B) holds. Otherwise, $w^{k\cdot\cdot} \models^c g$. If $w^k \Vdash c$, then the conclusion of (B) holds with $j = k$. Otherwise $w^k \not\Vdash c$. Since $\bar{w}^k \Vdash c$, it follows that $w^k = \bot$. Therefore, since w is proper, $w^{k\cdot\cdot} = \bot^\omega \models^c g$, a contradiction.

□

Remark: The implication

$$w \models^c \texttt{![!}g\ \texttt{U (!}f\ \texttt{\&\& !}g\texttt{)]} \quad \Longrightarrow \quad w \models^c \texttt{[}f\ \texttt{W}\ g\texttt{]}$$

may fail if $\bot^\omega \models^c g$. For example, let

$$\begin{aligned} f &= \text{TRUE} \\ g &= \texttt{!\{\{[*0]\} \&\& \{}\text{TRUE}\texttt{\}\}!} \\ w &= \bot^\omega \end{aligned}$$

Note that $w \not\models^c f$. Since

$$\top^\omega \not\models^c \texttt{\{\{[*0]\} \&\& \{}\text{TRUE}\texttt{\}\}!}$$

it follows that $w \models^c g$.

Referring to the conditions (A) and (B) in the proof of part 2 of Lemma 4.11, it follows that the precondition of (A) is always false, so (A) holds vacuously. However, (B) does not hold. To see this, note that the precondition of (B) is satisfied for any k: $\bar{w}^k = \top \models c$ and $w^{k\cdot\cdot} = w \not\models^c f$. But there does not exist j such that $w^j \models c$, so the conclusion of (B) fails. □

5 Rewrite rules

This section treats rewrite rules for clocked SEREs and formulas. For both SEREs and formulas, the semantic correspondence between a clocked entity and the rewritten unclocked entity is proved.

For reference, the rewrite rules from Appendix B of [1] are copied below.

Rewrite rules for SEREs:

- $\mathcal{R}^c(\{r\}) = \{\mathcal{R}^c(r)\}$
- $\mathcal{R}^c(b) = \{!c[*] \ ; \ c \ \&\& \ b\}$
- $\mathcal{R}^c(r_1 \ ; \ r_2) = \mathcal{R}^c(r_1) \ ; \ \mathcal{R}^c(r_2)$
- $\mathcal{R}^c(\{r_1\} \ : \ \{r_2\}) = \{\mathcal{R}^c(r_1)\} \ : \ \{\mathcal{R}^c(r_2)\}$
- $\mathcal{R}^c(\{r_1\} \ || \ \{r_2\}) = \{\mathcal{R}^c(r_1)\} \ || \ \{\mathcal{R}^c(r_2)\}$
- $\mathcal{R}^c(\{r_1\} \ \&\& \ \{r_2\}) = \{\mathcal{R}^c(r_1)\} \ \&\& \ \{\mathcal{R}^c(r_2)\}$
- $\mathcal{R}^c([*0]) = [*0]$
- $\mathcal{R}^c(r[*]) = \{\mathcal{R}^c(r)\}[*]$
- $\mathcal{R}^c(r \ @d) = \mathcal{R}^d(r)$

□

Rewrite rules for formulas:

- $\mathcal{F}^c((f)) = (\mathcal{F}^c(f))$
- $\mathcal{F}^c(b!) = [!c \ \mathtt{U} \ (c \ \&\& \ b)]$
- $\mathcal{F}^c(b) = [!c \ \mathtt{W} \ (c \ \&\& \ b)]$
- $\mathcal{F}^c(!f) = !\mathcal{F}^c(f)$
- $\mathcal{F}^c(f \ \&\& \ g) = \mathcal{F}^c(f) \ \&\& \ \mathcal{F}^c(g)$
- $\mathcal{F}^c(\mathtt{X!} \ f) = [!c \ \mathtt{U} \ (c \ \&\& \ \mathtt{X!} \ [!c \ \mathtt{U} \ (c \ \&\& \ \mathcal{F}^c(f))])]$
- $\mathcal{F}^c([f \ \mathtt{U} \ g]) = [(c \ \mathtt{->} \ \mathcal{F}^c(f)) \ \mathtt{U} \ (c \ \&\& \ \mathcal{F}^c(g))]$
- $\mathcal{F}^c(f \ \mathtt{abort} \ b) = \mathcal{F}^c(f) \ \mathtt{abort} \ b$
- $\mathcal{F}^c(f \ @d) = \mathcal{F}^d(f)$
- $\mathcal{F}^c(\{r\} \ \mathtt{|->} \ f) = \{\mathcal{R}^c(r)\} \ \mathtt{|->} \ \mathcal{F}^c(f)$
- $\mathcal{F}^c(\{r\}!) = \{\mathcal{R}^c(r)\}!$
- $\mathcal{F}^c(\{r\}) = \{\mathcal{R}^c(r)\}$

□

Lemma 5.1. *Let w be a finite word over Σ, let c be a boolean expression, and let r be a* SERE. *Then $w \models \mathcal{R}^c(r\,\texttt{[+]})$ iff $w \models \texttt{\{}\mathcal{R}^c(r)\texttt{\}[+]}$.*

Proof.

$$\begin{aligned}\mathcal{R}^c(r\,\texttt{[+]}) &= \mathcal{R}^c(r\ \texttt{;}\ r\,\texttt{[*]})\\ &= \mathcal{R}^c(r)\ \texttt{;}\ \mathcal{R}^c(r\,\texttt{[*]})\\ &= \mathcal{R}^c(r)\ \texttt{;}\ \texttt{\{}\mathcal{R}^c(r)\texttt{\}[*]}\end{aligned}$$

and

$$\texttt{\{}\mathcal{R}^c(r)\texttt{\}[+]} = \texttt{\{}\mathcal{R}^c(r)\texttt{\}}\ \texttt{;}\ \texttt{\{}\mathcal{R}^c(r)\texttt{\}[*]}$$

□

Lemma 5.2. *Let w be a finite word over Σ, let c be a boolean expression, and let r be a* SERE. *Then $w \models^c r$ iff $w \models \mathcal{R}^c(r)$.*

Proof. By induction over the structure of r.

- $r = \texttt{\{}r_1\texttt{\}}$.

  $w \models^c \texttt{\{}r_1\texttt{\}}$
  iff $w \models^c r_1$
  iff [induction]
  $w \models \mathcal{R}^c(r_1)$
  iff $w \models \texttt{\{}\mathcal{R}^c(r_1)\texttt{\}}$
  iff $w \models \mathcal{R}^c(\texttt{\{}r_1\texttt{\}})$

- $r = b$.

  $w \models^c b$
  iff w is a clock tick of c and $w^{|w|-1} \Vdash b$
  iff $|w| > 0$ and $w^{|w|-1} \Vdash c\ \texttt{\&\&}\ b$ and for all $0 \le i < |w| - 1$, $w^i \Vdash \texttt{!}c$
  iff $w \models \texttt{\{!}c\texttt{[*]}\ \texttt{;}\ c\ \texttt{\&\&}\ b\texttt{\}}$
  iff $w \models \mathcal{R}^c(b)$

- $r = r_1\ \texttt{;}\ r_2$.

  $w \models^c r_1\ \texttt{;}\ r_2$
  iff there exist u, v such that $w = uv$ and $u \models^c r_1$ and $v \models^c r_2$
  iff [induction]
  there exist u, v such that $w = uv$ and $u \models \mathcal{R}^c(r_1)$ and $v \models \mathcal{R}^c(r_2)$
  iff $w \models \mathcal{R}^c(r_1)\ \texttt{;}\ \mathcal{R}^c(r_2)$
  iff $w \models \mathcal{R}^c(r_1\ \texttt{;}\ r_2)$

- $r = \texttt{\{}r_1\texttt{\}}\ \texttt{:}\ \texttt{\{}r_2\texttt{\}}$.

$w \models^c \texttt{\{}r_1\texttt{\}} \texttt{ : } \texttt{\{}r_2\texttt{\}}$
iff there exist x, y, z such that $w = xyz$ and $|y| = 1$ and $xy \models^c r_1$ and $yz \models^c r_2$
iff [induction]
there exist x, y, z such that $w = xyz$ and $|y| = 1$ and $xy \models \mathcal{R}^c(r_1)$ and $yz \models \mathcal{R}^c(r_2)$
iff $w \models \texttt{\{}\mathcal{R}^c(r_1)\texttt{\}} \texttt{ : } \texttt{\{}\mathcal{R}^c(r_2)\texttt{\}}$
iff $w \models \mathcal{R}^c(\texttt{\{}r_1\texttt{\}} \texttt{ : } \texttt{\{}r_2\texttt{\}})$

- $r = \texttt{\{}r_1\texttt{\}} \texttt{ || } \texttt{\{}r_2\texttt{\}}$.

$w \models^c \texttt{\{}r_1\texttt{\}} \texttt{ || } \texttt{\{}r_2\texttt{\}}$
iff $w \models^c r_1$ or $w \models^c r_2$
iff [induction]
$w \models \mathcal{R}^c(r_1)$ or $w \models \mathcal{R}^c(r_2)$
iff $w \models \texttt{\{}\mathcal{R}^c(r_1)\texttt{\}} \texttt{ || } \texttt{\{}\mathcal{R}^c(r_2)\texttt{\}}$
iff $w \models \mathcal{R}^c(\texttt{\{}r_1\texttt{\}} \texttt{ || } \texttt{\{}r_2\texttt{\}})$

- $r = \texttt{\{}r_1\texttt{\}} \texttt{ \&\& } \texttt{\{}r_2\texttt{\}}$.

$w \models^c \texttt{\{}r_1\texttt{\}} \texttt{ \&\& } \texttt{\{}r_2\texttt{\}}$
iff $w \models^c r_1$ and $w \models^c r_2$
iff [induction]
$w \models \mathcal{R}^c(r_1)$ and $w \models \mathcal{R}^c(r_2)$
iff $w \models \texttt{\{}\mathcal{R}^c(r_1)\texttt{\}} \texttt{ \&\& } \texttt{\{}\mathcal{R}^c(r_2)\texttt{\}}$
iff $w \models \mathcal{R}^c(\texttt{\{}r_1\texttt{\}} \texttt{ \&\& } \texttt{\{}r_2\texttt{\}})$

- $r = \texttt{[*0]}$.

$w \models^c \texttt{[*0]}$
iff $|w| = 0$
iff $w \models \texttt{[*0]}$
iff $w \models \mathcal{R}^c(\texttt{[*0]})$

- $r = r_1\texttt{[*]}$.

$w \models^c r_1\texttt{[*]}$
iff [Lemma 3.4]
either
$w \models^c \texttt{[*0]}$
or
$w \models^c r_1\texttt{[+]}$
iff [Lemma 3.2]
either
$|w| = 0$
or
there exist $k > 0$ and $w_1, \ldots, w_k$ such that $w = w_1 \cdots w_k$ and $w_j \models^c r_1$ for each $1 \leq j \leq k$

iff [induction]
either
$w \models$ `[*0]`
or
there exist $k > 0$ and $w_1, \ldots, w_k$ such that $w = w_1 \cdots w_k$ and $w_j \models \mathcal{R}^c(r_1)$ for each $1 \leq j \leq k$
iff [Lemma 3.1]
either
$w \models$ `[*0]`
or
$w \models$ `{`$\mathcal{R}^c(r_1)$`}[+]`
iff [Lemma 3.3]
$w \models$ `{`$\mathcal{R}^c(r_1)$`}[*]`
iff $w \models \mathcal{R}^c(r_1$`[*]`$)$

- $r = r_1$ `@`d.

$w \models^c r_1$ `@`d
iff $w \models^d r_1$
iff [induction]
$w \models \mathcal{R}^d(r_1)$
iff $w \models \mathcal{R}^c(r_1$ `@`$d)$

□

Lemma 5.3. *Let w be a word over Σ, let c be a boolean expression, and let f be a PSL formula. Then $w \models^c f$ iff $w \models \mathcal{F}^c(f)$.*

Proof. By induction over the structure of f.

- $f =$ `(`g`)`.

$w \models^c$ `(`g`)`
iff $w \models^c g$
iff [induction]
$w \models \mathcal{F}^c(g)$
iff $w \models$ `(`$\mathcal{F}^c(g)$`)`
iff $w \models \mathcal{F}^c($`(`g`)`$)$

- $f = b$`!`.

$w \models^c b$`!`
iff there exists $0 \leq j < |w|$ such that $w^{0..j}$ is a clock tick of c and $w^j \not\models b$
iff there exists $0 \leq j < |w|$ such that $w^j \not\models c$ `&&` b and for all $0 \leq i < j$, $w^i \not\models$ `!`c
iff there exists $0 \leq j < |w|$ such that $w^{j..} \models c$ `&&` b and for all $0 \leq i < j$, $w^{i..} \models$ `!`c
iff $w \models$ `[!`c `U (`c `&&` b`)]`
iff $w \models \mathcal{F}^c(b$`!`$)$

- $f = b$.

  $w \models^c b$
  iff for all $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of c, $w^j \Vdash b$
  iff for all $0 \leq j < |w|$ such that $\bar{w}^j \Vdash c$, if for all $0 \leq i < j$, $\bar{w}^i \Vdash \texttt{!}c$, then $w^j \Vdash b$
  iff for all $0 \leq j < |w|$ such that $\bar{w}^j \Vdash c$, either there exists $0 \leq i < j$ such that $\bar{w}^i \not\Vdash \texttt{!}c$ or $w^j \Vdash b$
  iff [Lemma 3.5]
  (A):
  for all $0 \leq j < |w|$ such that $w^j \not\Vdash \texttt{!}c$,
  either
  1. there exists $0 \leq i < j$ such that $w^i \Vdash c$
  or
  2. $w^j \Vdash b$

  Let

  (B):
  for all $0 \leq j < |w|$ such that $w^j \not\Vdash \texttt{!}c$,
  either
  1. there exists $0 \leq i \leq j$ such that $w^i \Vdash c \texttt{ \&\& } b$
  or
  2. there exists $0 \leq i < j$ such that $w^i = \top$

  Assume (A). Let $0 \leq j' < |w|$ be such that $w^{j'} \not\Vdash \texttt{!}c$. Then either condition 1 or condition 2 of (A) holds with $j = j'$. If condition 2 holds, then $w^{j'} \notin \{\top, \bot\}$, hence $w^{j'} \Vdash c \texttt{ \&\& } b$, and so condition 1 of (B) holds. Suppose now that condition 1 of (A) holds, so there exists $0 \leq i' < j'$ such that $w^{i'} \Vdash c$. Without loss of generality, i' is minimal. If $w^{i'} = \top$, then plainly condition 2 of (B) holds. Otherwise, $w^{i'} \not\Vdash \texttt{!}c$. Then either condition 1 or condition 2 of (A) holds with $j = i'$. Condition 1 cannot hold because i' was chosen minimal. Therefore condition 2 holds, hence $w^{i'} \Vdash c \texttt{ \&\& } b$, and so condition 1 of (B) holds. This proves (B).

  Assume now (B). Let $0 \leq j' < |w|$ be such that $w^{j'} \not\Vdash \texttt{!}c$. Then either condition 1 or condition 2 of (B) holds with $j = j'$. If condition 2 holds, then plainly condition 1 of (A) holds. Suppose now that condition 1 of (B) holds, so there exists $0 \leq i' \leq j'$ such that $w^{i'} \Vdash c \texttt{ \&\& } b$. If $i' = j'$, then plainly condition 2 of (A) holds. If $i' < j'$, then plainly condition 1 of (A) holds. This proves (A) and completes the proof that (A) holds iff (B) holds.

  (B)
  iff for all $0 \leq j < |w|$ such that $w^{j..} \not\models \texttt{!}c$, either there exists $0 \leq i \leq j$ such that $w^{i..} \models c \texttt{ \&\& } b$ or there exists $0 \leq i < j$ such that $w^i = \top$
  iff [Lemma 4.8]
  $w \models \texttt{[!}c \texttt{ W (}c \texttt{ \&\& } b\texttt{)]}$
  iff $w \models \mathcal{F}^c(b)$

- $f = \texttt{!}g$.

  $w \models^c \texttt{!}g$
  iff $\bar{w} \not\models^c g$
  iff [induction]
  $\bar{w} \not\models \mathcal{F}^c(g)$
  iff $w \models \texttt{!}\mathcal{F}^c(g)$
  iff $w \models \mathcal{F}^c(\texttt{!}g)$

- $f = g \texttt{ \&\& } h$.

  $w \models^c g \texttt{ \&\& } h$
  iff $w \models^c g$ and $w \models^c h$
  iff [induction]
  $w \models \mathcal{F}^c(g)$ and $w \models \mathcal{F}^c(h)$
  iff $w \models \mathcal{F}^c(g) \texttt{ \&\& } \mathcal{F}^c(h)$
  iff $w \models \mathcal{F}^c(g \texttt{ \&\& } h)$

- $f = \texttt{X! } g$.

  $w \models^c \texttt{X! } g$
  iff there exist $0 \leq j < k < |w|$ such that $w^{0..j}$ and $w^{j+1..k}$ are clock ticks of c and $w^{k..} \models^c g$
  iff [induction]
  there exist $0 \leq j < k < |w|$ such that $w^{0..j}$ and $w^{j+1..k}$ are clock ticks of c and $w^{k..} \models \mathcal{F}^c(g)$
  iff there exist $0 \leq j < k < |w|$ such that $w^{k..} \models \mathcal{F}^c(g)$ and $w^k \Vdash c$ and $w^j \Vdash c$ and for all i such that $0 \leq i < j$ or $j < i < k$, $w^i \Vdash \texttt{!}c$
  iff there exist $0 \leq j < |w| - 1$ such that $w^{j+1..} \models \texttt{[!}c \texttt{ U (}c \texttt{ \&\& } \mathcal{F}^c(g)\texttt{)]}$ and $w^j \Vdash c$ and for all $0 \leq i < j$, $w^i \Vdash \texttt{!}c$
  iff there exist $0 \leq j < |w|$ such that $w^{j..} \models \texttt{X! [!}c \texttt{ U (}c \texttt{ \&\& } \mathcal{F}^c(g)\texttt{)]}$ and $w^j \Vdash c$ and for all $0 \leq i < j$, $w^i \Vdash \texttt{!}c$
  iff $w \models \texttt{[!}c \texttt{ U (}c \texttt{ \&\& X! [!}c \texttt{ U (}c \texttt{ \&\& } \mathcal{F}^c(g)\texttt{)])]}$
  iff $w \models \mathcal{F}^c(\texttt{X! } g)$

- $f = \texttt{[}g \texttt{ U } h\texttt{]}$.

  $w \models^c \texttt{[}g \texttt{ U } h\texttt{]}$
  iff there exists $0 \leq k < |w|$ such that $w^k \Vdash c$ and $w^{k..} \models^c h$ and for all $0 \leq j < k$ such that $\bar{w}^j \Vdash c$, $w^{j..} \models^c g$
  iff [induction]
  there exists $0 \leq k < |w|$ such that $w^k \Vdash c$ and $w^{k..} \models \mathcal{F}^c(h)$ and for all $0 \leq j < k$ such that $\bar{w}^j \Vdash c$, $w^{j..} \models \mathcal{F}^c(g)$
  iff there exists $0 \leq k < |w|$ such that $w^{k..} \models c \texttt{ \&\& } \mathcal{F}^c(h)$ and for all $0 \leq j < k$, either $\bar{w}^j \not\Vdash c$ or $w^{j..} \models \mathcal{F}^c(g)$
  iff [Lemma 3.5]
  there exists $0 \leq k < |w|$ such that $w^{k..} \models c \texttt{ \&\& } \mathcal{F}^c(h)$ and for all

$0 \le j < k$, either $w^j \not\models \texttt{!}c$ or $w^{j\cdot\cdot} \models \mathcal{F}^c(g)$
iff there exists $0 \le k < |w|$ such that $w^{k\cdot\cdot} \models c \texttt{ \&\& } \mathcal{F}^c(h)$ and for all $0 \le j < k$, $w^{j\cdot\cdot} \models c \texttt{ -> } \mathcal{F}^c(g)$
iff $w \models \texttt{[(}c \texttt{ -> } \mathcal{F}^c(g)\texttt{) U (}c \texttt{ \&\& } \mathcal{F}^c(h)\texttt{)]}$
iff $w \models \mathcal{F}^c(\texttt{[}g \texttt{ U } h\texttt{]})$

- $f = g \texttt{ abort } b$.

  $w \models^c g \texttt{ abort } b$
  iff either $w \models^c g$ or there exists $0 \le j < |w|$ such that $w^j \not\models b$ and $w^{0..j-1}\top^\omega \models^c g$
  iff [induction]
  either $w \models \mathcal{F}^c(g)$ or there exists $0 \le j < |w|$ such that $w^j \not\models b$ and $w^{0..j-1}\top^\omega \models \mathcal{F}^c(g)$
  iff $w \models \mathcal{F}^c(g) \texttt{ abort } b$
  iff $w \models \mathcal{F}^c(g \texttt{ abort } b)$

- $f = g \texttt{ @}d$.

  $w \models^c g \texttt{ @}d$
  iff $w \models^d g$
  iff [induction]
  $w \models \mathcal{F}^d(g)$
  iff $w \models \mathcal{F}^c(g \texttt{ @}d)$

- $f = \texttt{\{}r\texttt{\} |-> } g$.

  $w \models^c \texttt{\{}r\texttt{\} |-> } g$
  iff for all $0 \le j < |w|$ such that $\bar{w}^{0..j} \not\models^c r$, $w^{j\cdot\cdot} \models^c g$
  iff [induction, Lemma 5.2]
  for all $0 \le j < |w|$ such that $\bar{w}^{0..j} \not\models \mathcal{R}^c(r)$, $w^{j\cdot\cdot} \models \mathcal{F}^c(g)$
  iff $w \models \texttt{\{}\mathcal{R}^c(r)\texttt{\} |-> } \mathcal{F}^c(g)$
  iff $w \models \mathcal{F}^c(\texttt{\{}r\texttt{\} |-> } g)$

- $f = \texttt{\{}r\texttt{\}!}$.

  $w \models^c \texttt{\{}r\texttt{\}!}$
  iff there exists $0 \le j < |w|$ such that $w^{0..j} \not\models^c r$
  iff [Lemma 5.2]
  there exists $0 \le j < |w|$ such that $w^{0..j} \not\models \mathcal{R}^c(r)$
  iff $w \models \texttt{\{}\mathcal{R}^c(r)\texttt{\}!}$
  iff $w \models \mathcal{F}^c(\texttt{\{}r\texttt{\}!})$

- $f = \texttt{\{}r\texttt{\}}$.

  $w \models^c \texttt{\{}r\texttt{\}}$
  iff for all $0 \le j < |w|$, $w^{0..j}\top^\omega \models^c \texttt{\{}r\texttt{\}!}$
  iff [argument for $f = \texttt{\{}r\texttt{\}!}$]

$$
\begin{array}{ll}
 & \text{for all } 0 \leq j < |w|,\ w^{0..j}\top^\omega \models \mathcal{F}^c(\{r\}!) \\
\text{iff} & \text{for all } 0 \leq j < |w|,\ w^{0..j}\top^\omega \models \{\mathcal{R}^c(r)\}! \\
\text{iff} & w \models \{\mathcal{R}^c(r)\} \\
\text{iff} & w \models \mathcal{F}^c(\{r\})
\end{array}
$$

□

Corollary 5.4. *Let w be a word over Σ, let c be a boolean expression, and let f be a PSL formula.*

1. $w \models^{c-} f$ *iff* $w \models^{-} \mathcal{F}^c(f)$.
2. $w \models^{c+} f$ *iff* $w \models^{+} \mathcal{F}^c(f)$.

□

6 Clock ticks

Lemma 6.1. *Let w be a finite word over Σ. w is a clock tick of* TRUE *iff there exist $k \geq 0$ and $a \neq \bot$ such that $w = \top^k a$.*

Proof.

w is a clock tick of TRUE
iff $|w| > 0$ and $w^{|w|-1} \models$ TRUE and for every $0 \leq i < |w| - 1$, $w^i \models$ FALSE
iff $|w| > 0$ and $w^{|w|-1} \neq \bot$ and for every $0 \leq i < |w| - 1$, $w^i = \top$
iff [let $k = |w| - 1$, $a = w^{|w|-1}$]
there exists $k \geq 0$ and $a \neq \bot$ such that $w = \top^k a$

□

Lemma 6.2. *Let c be a boolean expression. Then $\top^k$ is a clock tick of c iff $k > 0$.*

Proof.

$\top^k$ is a clock tick of c
iff $|\top^k| > 0$ and $\top \models c$ and for all $0 \leq i < k - 1$, $\top \models !c$
iff [$\top$ satisfies all boolean expressions]
$k > 0$

□

7 Tight satisfaction of SEREs

This section presents results on the unclocked and clocked tight satisfaction relations.

The rewrite rules for SEREs and Lemma 5.2 show that the clocked tight satisfaction relation can be derived from the unclocked tight satisfaction relation. The unclocked tight-satisfaction semantics of unclocked SEREs is related to the clocked tight-satisfaction semantics of unclocked SEREs clocked by TRUE, but the two semantics are not equivalent.

Lemma 7.1. *Let w be a finite word over Σ and let r be an unclocked* SERE. *If $w \models r$, then $w \models^{\text{TRUE}} r$.*

Proof. By induction over the structure of r. Note that for each of the primitive unclocked SERE forms except boolean expression, the corresponding clocked SERE definition is obtained by changing $\models$ to $\models^c$. Therefore it is enough to check the implication in the case of boolean expressions.

$w \models b$
iff $|w| = 1$ and $w^0 \models b$
iff $w = \top^0 w^0$ and $w^0 \neq \bot$ and $w^0 \models b$
$\Rightarrow$ [Lemma 6.1]
w is a clock tick of TRUE and $w^{|w|-1} \models b$
iff $w \models^{\text{TRUE}} b$

□

Remark: The converse of the preceding lemma does not hold. For example, $\top^2 \models^{\text{TRUE}}$ TRUE, but $\top^2 \not\models$ TRUE. The converse does hold if w is a word over $2^{\mathbf{P}}$. Therefore, for words over $2^{\mathbf{P}}$, the unclocked tight-satisfaction semantics of unclocked SEREs can be derived as a special case of the clocked tight-satisfaction semantics of unclocked SEREs clocked at TRUE. However, for general words over Σ, the PSL unclocked tight-satisfaction semantics of unclocked SEREs is not derived in this way. □

Lemma 7.2. *Let w be a finite word over Σ, and let r be an unclocked* SERE. *If $w \models r$, then no letter of w is $\bot$.*

Proof. By induction over the structure of r. Write $good(w)$ to mean that no letter of w is $\bot$.

- $r = b$.

  $w \models b$
  iff $|w| = 1$ and $w^0 \models b$
  $\Rightarrow$ $|w| = 1$ and $w^0 \neq \bot$
  $\Rightarrow$ $good(w)$

- $r = \{r_1\}$.

$w \models$ `{`r_1`}`
iff $w \models r_1$
$\Rightarrow$ [induction]
$good(w)$

- $r = r_1$ `;` r_2.

  $w \models r_1$ `;` r_2
  iff there exist u, v such that $w = uv$ and $u \models r_1$ and $v \models r_2$
  $\Rightarrow$ [induction]
  there exist u, v such that $w = uv$ and $good(u)$ and $good(v)$
  $\Rightarrow$ $good(w)$

- $r =$ `{`r_1`}` `:` `{`r_2`}`.

  $w \models$ `{`r_1`}` `:` `{`r_2`}`
  iff there exist x, y, z such that $w = xyz$ and $|y| = 1$ and $xy \models r_1$ and
  $yz \models r_2$
  $\Rightarrow$ [induction]
  there exist x, y, z such that $w = xyz$ and $good(xy)$ and $good(yz)$
  $\Rightarrow$ $good(w)$

- $r =$ `{`r_1`}` `||` `{`r_2`}`.

  $w \models$ `{`r_1`}` `||` `{`r_2`}`
  iff $w \models r_1$ or $w \models r_2$
  $\Rightarrow$ [induction]
  $good(w)$ or $good(w)$
  iff $good(w)$

- $r =$ `{`r_1`}` `&&` `{`r_2`}`.

  $w \models$ `{`r_1`}` `&&` `{`r_2`}`
  iff $w \models r_1$ and $w \models r_2$
  $\Rightarrow$ [induction]
  $good(w)$ and $good(w)$
  iff $good(w)$

- $r =$ `[*0]`.

  $w \models$ `[*0]`
  iff $|w| = 0$
  $\Rightarrow$ $good(w)$

- $r = r_1$`[+]`.

$w \models r_1\texttt{[+]}$
iff [Lemma 3.1]
there exist $k > 0$ and $w_1, \ldots, w_k$ such that $w = w_1 \cdots w_k$ and $w_j \models r_1$ for all $1 \leq j \leq k$
$\Rightarrow$ [induction]
there exist $k > 0$ and $w_1, \ldots, w_k$ such that $w = w_1 \cdots w_k$ and $\mathit{good}(w_j)$ for all $1 \leq j \leq k$
$\Rightarrow$ $\mathit{good}(w)$

□

Lemma 7.3. *Let w be a finite word over Σ, let r be a* SERE*, and let c be a boolean expression. If $w \models^c r$, then no letter of w is $\bot$.*

Proof.

$w \models^c r$
iff [Lemma 5.2]
$w \models \mathcal{R}^c(r)$
$\Rightarrow$ [Lemma 7.2]
no letter of w is $\bot$

□

Lemma 7.4. *Let r be an unclocked* SERE*, let w be a finite word over Σ, and let t be a finite word over Σ such that $|t| = |w|$ and such that for all $0 \leq i < |w|$, either $t^i = w^i$ or $t^i = \top$. If $w \models r$, then $t \models r$.*

Proof. By induction over the structure of r.

- $r = b$.

  $w \models b$
  iff $|w| = 1$ and $w^0 \models b$
  $\Rightarrow$ [$|t| = |w|$ and either $t^0 = w^0$ or $t^0 = \top$]
  $|t| = 1$ and $t^0 \models b$
  iff $t \models b$

- $r = \{r_1\}$.

  $w \models \{r_1\}$
  iff $w \models r_1$
  $\Rightarrow$ [induction]
  $t \models r_1$
  iff $t \models \{r_1\}$

- $r = r_1 \ ; \ r_2$.

  Assume $w \models r_1 \ ; \ r_2$. Then there exist u, v such that $w = uv$ and $u \models r_1$ and $v \models r_2$. Then there exist t_u, t_v such that $|t_u| = |u|$ and $|t_v| = |v|$ and $t = t_u t_v$. By induction, $t_u \models r_1$ and $t_v \models r_2$. Therefore $t \models r_1 \ ; \ r_2$.

- $r = \{r_1\} : \{r_2\}$.

  Assume $w \models\!\equiv \{r_1\} : \{r_2\}$. Then there exist x, y, z such that $w = xyz$ and $|y| = 1$ and $xy \models\!\equiv r_1$ and $yz \models\!\equiv r_2$. Then there exist t_x, t_y, t_z such that $|t_x| = |x|$ and $|t_y| = |y|$ and $|t_z| = |z|$ and $t = t_x t_y t_z$. By induction, $t_x t_y \models\!\equiv r_1$ and $t_y t_z \models\!\equiv r_2$. Therefore $t \models\!\equiv \{r_1\} : \{r_2\}$.

- $r = \{r_1\} \texttt{||} \{r_2\}$.

  $w \models\!\equiv \{r_1\} \texttt{||} \{r_2\}$
  iff $w \models\!\equiv r_1$ or $w \models\!\equiv r_2$
  $\Rightarrow$ [induction]
  $t \models\!\equiv r_1$ or $t \models\!\equiv r_2$
  iff $t \models\!\equiv \{r_1\} \texttt{||} \{r_2\}$

- $r = \{r_1\} \texttt{\&\&} \{r_2\}$.

  $w \models\!\equiv \{r_1\} \texttt{\&\&} \{r_2\}$
  iff $w \models\!\equiv r_1$ and $w \models\!\equiv r_2$
  $\Rightarrow$ [induction]
  $t \models\!\equiv r_1$ and $t \models\!\equiv r_2$
  iff $t \models\!\equiv \{r_1\} \texttt{\&\&} \{r_2\}$

- $r = \texttt{[*0]}$.

  $w \models\!\equiv \texttt{[*0]}$
  iff $|w| = 0$
  $\Rightarrow$ $|t| = 0$
  iff $t \models\!\equiv \texttt{[*0]}$

- $r = r_1\texttt{[+]}$.

  Assume $w \models\!\equiv r_1\texttt{[+]}$. By Lemma 3.1, there exist $k > 0$ and $w_1, \ldots, w_k$ such that $w = w_1 \cdots w_k$ and $w_j \models\!\equiv r_1$ for all $1 \leq j \leq k$. Then there exist $t_1, \ldots, t_k$ such that $|t_j| = |w_j|$ for all $1 \leq j \leq k$ and such that $t = t_1 \cdots t_k$. By induction, $t_j \models\!\equiv r_1$ for all $1 \leq j \leq k$, and so $t \models\!\equiv r_1\texttt{[+]}$.

□

Lemma 7.5. *Let r be a* SERE*, let c be a boolean expression, let w be a finite word over Σ, and let t be a finite word over Σ such that $|t| = |w|$ and such that for all $0 \leq i < |w|$, either $t^i = w^i$ or $t^i = \top$. If $w \models\!\equiv^c r$, then $t \models\!\equiv^c r$.*

Proof.

$w \models\!\equiv^c r$
iff [Lemma 5.2]
$w \models\!\equiv \mathcal{R}^c(r)$
$\Rightarrow$ [Lemma 7.4]
$t \models\!\equiv \mathcal{R}^c(r)$
iff [Lemma 5.2]
$t \models\!\equiv^c r$

□

Remark: Note that t can be taken as $\top^{|w|}$ in Lemma 7.4 and Lemma 7.5. □

Lemma 7.6. *Let r be a* SERE*, and let c be a boolean expression. Then $\top^k \models^c r$ iff $\top^k \models^{\text{TRUE}} r$.*

Proof. By induction over the structure of r. Let $t = \top^k$.

- $r = b$.

  $t \models^c b$
  iff t is a clock tick of c and $t^{|t|-1} \models b$
  iff [Lemma 6.2]
  $k > 0$ and $t^{|t|-1} \models b$
  iff [Lemma 6.2]
  t is a clock tick of TRUE and $t^{|t|-1} \models b$
  iff $t \models^{\text{TRUE}} b$

- $r = \{r_1\}$.

  $t \models^c \{r_1\}$
  iff $t \models^c r_1$
  iff [induction]
  $t \models^{\text{TRUE}} r_1$
  iff $t \models^{\text{TRUE}} \{r_1\}$

- $r = r_1 \ ; \ r_2$.

  $t \models^c r_1 \ ; \ r_2$
  iff there exist u, v such that $t = uv$ and $u \models^c r_1$ and $v \models^c r_2$
  iff [induction, using $u = \top^{|u|}$, $v = \top^{|v|}$]
  there exist u, v such that $t = uv$ and $u \models^{\text{TRUE}} r_1$ and $v \models^{\text{TRUE}} r_2$
  iff $t \models^{\text{TRUE}} r_1 \ ; \ r_2$

- $r = \{r_1\} : \{r_2\}$.

  $t \models^c \{r_1\} : \{r_2\}$
  iff there exist x, y, z such that $t = xyz$ and $|y| = 1$ and
  $xy \models^c r_1$ and $yz \models^c r_2$
  iff [induction, using $xy = \top^{|xy|}$, $yz = \top^{|yz|}$]
  there exist x, y, z such that $t = xyz$ and $|y| = 1$ and
  $xy \models^{\text{TRUE}} r_1$ and $yz \models^{\text{TRUE}} r_2$
  iff $t \models^{\text{TRUE}} \{r_1\} : \{r_2\}$

- $r = \{r_1\} \ || \ \{r_2\}$.

$t \models^c$ `{`r_1`} || {`r_2`}`
iff $t \models^c r_1$ or $t \models^c r_2$
iff [induction]
$t \models^{\text{TRUE}} r_1$ or $t \models^{\text{TRUE}} r_2$
iff $t \models^{\text{TRUE}}$ `{`r_1`} || {`r_2`}`

- $r =$ `{`r_1`} && {`r_2`}`.

$t \models^c$ `{`r_1`} && {`r_2`}`
iff $t \models^c r_1$ and $t \models^c r_2$
iff [induction]
$t \models^{\text{TRUE}} r_1$ and $t \models^{\text{TRUE}} r_2$
iff $t \models^{\text{TRUE}}$ `{`r_1`} && {`r_2`}`

- $r =$ `[*0]`.

$t \models^c$ `[*0]`
iff $|t| = 0$
iff $t \models^{\text{TRUE}}$ `[*0]`

- $r = r_1$`[+]`.

$t \models^c r_1$`[+]`
iff [Lemma 3.2]
there exist $k > 0$ and $t_1, \ldots, t_k$ such that $t = t_1 \cdots t_k$ and
$t_j \models^c r_1$ for all $1 \leq j \leq k$
iff [induction]
there exist $k > 0$ and $t_1, \ldots, t_k$ such that $t = t_1 \cdots t_k$ and
$t_j \models^{\text{TRUE}} r_1$ for all $1 \leq j \leq k$
iff [Lemma 3.2]
$t \models^{\text{TRUE}} r_1$`[+]`

- $r = r_1$ `@`d.

$t \models^c r_1$ `@`d
iff $t \models^d r_1$
iff $t \models^{\text{TRUE}} r_1$ `@`d

□

Lemma 7.7. *Let r be an unclocked* SERE*, let c be a boolean expression, and let w be a non-empty finite word over Σ. If $w \models^c r$, then $w^{|w|-1} \models c$.*

Proof. By induction over the structure of r. Let $I = |w| - 1$.

- $r = b$.

$w \models^c b$
iff w is a clock tick of c and $w^{|w|-1} \models b$
iff $|w| > 0$, $w^j \models \,!c$ for all $0 \leq j < |w| - 1$, and $w^{|w|-1} \models c$ and $w^{|w|-1} \models b$
$\Rightarrow$ $w^I \models c$

- $r = \{r_1\}$.

  $w \models^c \{r_1\}$
  iff $w \models^c r_1$
  $\Rightarrow$ [induction]
  $w^I \models c$

- $r = r_1 \ ; \ r_2$.

  $w \models^c r_1 \ ; \ r_2$
  iff there exist u, v such that $w = uv$ and $u \models^c r_1$ and $v \models^c r_2$
  $\Rightarrow$ [induction]
  $w = uv$ and if u is non-empty then $u^{|u|-1} \models c$ and if v is non-empty then $v^{|v|-1} \models c$
  $\Rightarrow$ [$w = uv$ is non-empty; if $|v| > 0$ then $w^I = v^{|v|-1}$; otherwise $w^I = u^{|u|-1}$]
  $w^I \models c$

- $r = \{r_1\} \ : \ \{r_2\}$.

  $w \models^c \{r_1\} \ : \ \{r_2\}$
  iff there exist x, y, z such that $w = xyz$ and $|y| = 1$ and $xy \models^c r_1$ and $yz \models^c r_2$
  $\Rightarrow$ [induction]
  $w = xyz$ and $yz^{|yz|-1} \models c$
  $\Rightarrow$ [$w^I = yz^{|yz|-1}$]
  $w^I \models c$

- $r = \{r_1\} \ || \ \{r_2\}$.

  $w \models^c \{r_1\} \ || \ \{r_2\}$
  iff $w \models^c r_1$ or $w \models^c r_2$
  $\Rightarrow$ [induction]
  $w^I \models c$ or $w^I \models c$
  iff $w^I \models c$

- $r = \{r_1\} \ \&\& \ \{r_2\}$.

$w \models^c$ `{`r_1`} && {`r_2`}`
iff $w \models^c r_1$ and $w \models^c r_2$
$\Rightarrow$ [induction]
$w^I \models c$ and $w^I \models c$
iff $w^I \models c$

- $r =$ `[*0]`. Since w is non-empty, $w \not\models^c$ `[*0]`.
- $r = r_1$`[+]`.

$w \models^c r_1$`[+]`
iff [Lemma 3.2]
there exist $k > 0$ and $w_1, \ldots, w_k$ such that $w = w_1 \cdots w_k$ and $w_j \models^c r_1$ for all $1 \leq j \leq k$
iff [throw away unnecessary empty w_j and reindex]
there exist $k > 0$ and non-empty $w_1, \ldots, w_k$ such that $w = w_1 \cdots w_k$ and $w_j \models^c r_1$ for all $1 \leq j \leq k$
$\Rightarrow$ [induction]
there exist $k > 0$ and non-empty $w_1, \ldots, w_k$ such that $w = w_1 \cdots w_k$ and $w_j^{|w_j|-1} \models c$ all $1 \leq j \leq k$
$\Rightarrow$ [$w^I = w_k^{|w_k|-1}$]
$w^I \models c$

□

8 SERE formulas

Let r be a SERE. The strong promotion of r to a PSL formula is denoted $\{r\}!$, while the weak promotion is denoted $\{r\}$. This section presents results on the formula semantics of $\{r\}!$ and $\{r\}$.

Lemma 8.1. *Let w be a word over Σ, let c be a boolean expression, and let r be a* SERE*.*

1. $w \models^c \{r\}!$ *iff* $w \models \{\mathcal{R}^c(r)\}!$.

2. $w \models^c \{r\}$ *iff* $w \models \{\mathcal{R}^c(r)\}$.

Proof. Immediate from Lemma 5.3 and the rewrite rules. □

Lemma 8.2. *Let w be a word over Σ, let c be a boolean expression, and let r be a* SERE*.*

1. $w \models^{c-} \{r\}!$ *iff* $w \models^- \{\mathcal{R}^c(r)\}!$.

2. $w \models^{c-} \{r\}$ *iff* $w \models^- \{\mathcal{R}^c(r)\}$.

3. $w \models^{c+} \{r\}!$ *iff* $w \models^+ \{\mathcal{R}^c(r)\}!$.

4. $w \models^{c+} \{r\}$ *iff* $w \models^+ \{\mathcal{R}^c(r)\}$.

Proof. Immediate from Corollary 5.4 and the rewrite rules. □

Lemma 8.3. *Let w be a word over Σ, let c be a boolean expression, and let r be an unclocked* SERE*.*

1. $w \models \{r\}!$ *iff* $w \models !(\{r\} \mid\!\!-> \text{FALSE})$.

2. $w \models^c \{r\}!$ *iff* $w \models^c !(\{r\} \mid\!\!-> \text{FALSE})$

Proof.

1. $w \models !(\{r\} \mid\!\!-> \text{FALSE})$
   iff $\bar{w} \not\models \{r\} \mid\!\!-> \text{FALSE}$
   iff $\neg$(for every $0 \le j < |w|$ such that $w^{0..j} \models r$, $\bar{w}^{j..} \models \text{FALSE}$)
   iff there exists $0 \le j < |w|$ such that $w^{0..j} \models r$ and $\bar{w}^{j..} \not\models \text{FALSE}$
   iff [if $0 \le j < |w|$, then $\bar{w}^{j..}$ is non-empty]
   there exists $0 \le j < |w|$ such that $w^{0..j} \models r$ and $\bar{w}^{j} \not\models \text{FALSE}$
   iff there exists $0 \le j < |w|$ such that $w^{0..j} \models r$ and $\bar{w}^j \neq \top$
   iff there exists $0 \le j < |w|$ such that $w^{0..j} \models r$ and $w^j \neq \bot$
   iff [if $w^{0..j} \models r$, then $w^j \neq \bot$ by Lemma 7.2]
   there exists $0 \le j < |w|$ such that $w^{0..j} \models r$

2. $w \models^c$ `!({r} |->` FALSE`)`
   iff $\bar{w} \not\models^c$ `{r} |->` FALSE
   iff $\neg$(for every $0 \leq j < |w|$ such that $w^{0..j} \models^c r$, $\bar{w}^{j..} \models^c$ FALSE)
   iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models^c r$ and $\bar{w}^{j..} \not\models^c$ FALSE
   iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models^c r$ and $\neg$(for all $j \leq k < |w|$ such that $w^{j..k}$ is a clock tick of c, then $\bar{w}^k \not\models$ FALSE)
   iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models^c r$ and there exists $j \leq k < |w|$ such that $w^{j..k}$ is a clock tick of c and $\bar{w}^k \not\models$ FALSE
   iff [if $w^{j..k}$ is a clock tick of c, then $w^k \not\models c$, hence $w^k \neq \bot$, hence $\bar{w}^k \neq \top$, hence $\bar{w}^k \not\models$ FALSE]
   there exists $0 \leq j < |w|$ such that $w^{0..j} \models^c r$ and there exists $j \leq k < |w|$ such that $w^{j..k}$ is a clock tick of c
   iff [if $w^{0..j} \models^c r$, then, by Lemma 7.7, $w^j \not\models c$, hence $w^{j..j}$ is a clock tick of c]
   there exists $0 \leq j < |w|$ such that $w^{0..j} \models^c r$

□

Lemma 8.4. *Let r be a* SERE*, let c be a boolean expression, and let w be a word over Σ. Then $w \models^c$ `{r}!` iff $w \models^c$ `!({r} |->` FALSE `@`TRUE`)`.*

Proof.

$w \models^c$ `!({r} |->` FALSE `@`TRUE`)`
iff $\bar{w} \not\models^c$ `{r} |->` FALSE `@`TRUE
iff $\neg$(for every $0 \leq j < |w|$ such that $w^{0..j} \models^c r$, $\bar{w}^{j..} \models^c$ FALSE `@`TRUE)
iff $\neg$(for every $0 \leq j < |w|$ such that $w^{0..j} \models^c r$, $\bar{w}^{j..} \models^{\text{TRUE}}$ FALSE)
iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models^c r$ and $\neg(\bar{w}^{j..} \models^{\text{TRUE}}$ FALSE)
iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models^c r$ and $\neg$(for all $j \leq k < |w|$ such that $w^{j..k}$ is a clock tick of TRUE, $\bar{w}^k \not\models$ FALSE)
iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models^c r$ and there exists $j \leq k < |w|$ such that $w^{j..k}$ is a clock tick of TRUE and $\bar{w}^k \not\models$ FALSE
iff [if $w^{j..k}$ is a clock tick of TRUE, then $w^k \not\models$ TRUE, hence $w^k \neq \bot$, hence $\bar{w}^k \neq \top$, hence $\bar{w}^k \not\models$ FALSE]
there exists $0 \leq j < |w|$ such that $w^{0..j} \models^c r$ and there exists $j \leq k < |w|$ such that $w^{j..k}$ is a clock tick of TRUE
iff [if $w^{0..j} \models^c r$, then $w^j \neq \bot$, so $w^{j..j}$ is a clock tick of TRUE]
there exists $0 \leq j < |w|$ such that $w^{0..j} \models^c r$

□

Lemma 8.5. *Let w be a word over Σ, and let r be an unclocked* SERE*. The following are equivalent:*

1. $w \models$ `{r}`.

2. *For every non-empty finite $u \preceq w$, $u \models^-$ `{r}!`.*

3. $|w| = 0$ *or for every finite $u \preceq w$, $u \models^-$ `{r}!`.*

Proof.

$w \models \{r\}$
iff for all $0 \leq j < |w|$, $w^{0..j}\top^\omega \models \{r\}!$
iff for every non-empty finite $u \preceq w$, $u \models^- \{r\}!$

$w \models \{r\}$
iff for all $0 \leq j < |w|$, $w^{0..j}\top^\omega \models \{r\}!$
iff $|w| = 0$ or ($|w| > 0$ and for all $0 \leq j < |w|$, $w^{0..j}\top^\omega \models \{r\}!$)
iff [by Lemma 7.4, if $w^{0..0}\top^\omega \models \{r\}!$, then $\top^\omega \models \{r\}!$]
$|w| = 0$ or ($|w| > 0$ and for every finite $u \preceq w$, $u\top^\omega \models \{r\}!$)
iff $|w| = 0$ or for every finite $u \preceq w$, $u \models^- \{r\}!$

□

Lemma 8.6. *Let w be a word over Σ, let c be a boolean expression, and let r be a* SERE. *The following are equivalent:*

1. $w \models^c \{r\}$.

2. *For every non-empty finite $u \preceq w$, $u \models^{c-} \{r\}!$.*

3. *$|w| = 0$ or for every finite $u \preceq w$, $u \models^{c-} \{r\}!$.*

Proof. Follows from Lemma 8.5 using Lemma 8.1 and Lemma 8.2. □

Lemma 8.7. *Let w be a word over Σ, and let r be an unclocked* SERE. *If $w \models \{r\}!$, then $w \models \{r\}$.*

Proof. Assume $w \models \{r\}!$. Then there exists $0 \leq k < |w|$ such that $w^{0..k} \models r$. In particular, $|w| > 0$. Let u be any finite prefix of w. By Lemma 7.4, $(u\top^\omega)^{0..k} \models r$. Therefore $u\top^\omega \models \{r\}!$. By Lemma 8.5, this proves that $w \models \{r\}$. □

Lemma 8.8. *Let w be a word over Σ, let c be a boolean expression, and let r be a* SERE. *If $w \models^c \{r\}!$, then $w \models^c \{r\}$.*

Proof. Follows from Lemma 8.7 using Lemma 8.1. □

Lemma 8.9. *Let w be a finite word over Σ, and let r be an unclocked* SERE.

1. *The following are equivalent:*

- $w \models^- \{r\}$.
- $w \models^- \{r\}!$.
- *For every finite $u \preceq w$, $u \models^- \{r\}!$.*

2. *The following are equivalent:*

- $w \models^+ \{r\}$
- $w \models^+ \{r\}!$

- $w \models \texttt{\{}r\texttt{\}!}$

Proof.

1. Note that

   $w \models^{-} \texttt{\{}r\texttt{\}}$
   iff $w\top^\omega \models \texttt{\{}r\texttt{\}}$
   iff [Lemma 8.5; $|w\top^\omega| > 0$]
   for every finite $u \preceq w\top^\omega$, $u\top^\omega \models \texttt{\{}r\texttt{\}!}$
   iff for every finite $u \preceq w$, $u\top^\omega \models \texttt{\{}r\texttt{\}!}$
   iff for every finite $u \preceq w$, $u \models^{-} \texttt{\{}r\texttt{\}!}$

   Then

   $w \models^{-} \texttt{\{}r\texttt{\}}$
   $\Rightarrow$ [since w is finite, let $u = w$]
   $w \models^{-} \texttt{\{}r\texttt{\}!}$

   and

   $w \models^{-} \texttt{\{}r\texttt{\}!}$
   iff $w\top^\omega \models \texttt{\{}r\texttt{\}!}$
   iff there exists $j \geq 0$ such that $(w\top^\omega)^{0..j} \models\!\models r$
   $\Rightarrow$ [Lemma 7.4]
   there exists $j \geq 0$ such that for every finite $u \preceq w$, $(u\top^\omega)^{0..j} \models\!\models r$
   $\Rightarrow$ for every finite $u \preceq w$, $u\top^\omega \models \texttt{\{}r\texttt{\}!}$
   iff for every finite $u \preceq w$, $u \models^{-} \texttt{\{}r\texttt{\}!}$
   $\Rightarrow$ [Lemma 8.5]
   $w \models^{-} \texttt{\{}r\texttt{\}}$

2. Note that

   $w \models^{+} \texttt{\{}r\texttt{\}!}$
   iff $w\bot^\omega \models \texttt{\{}r\texttt{\}!}$
   iff there exists $j \geq 0$ such that $(w\bot^\omega)^{0..j} \models\!\models r$
   iff [Lemma 7.2]
   there exists $0 \leq j < |w|$ such that $w^{0..j} \models\!\models r$
   iff $w \models \texttt{\{}r\texttt{\}!}$

   By Lemma 8.7, $w \models^{+} \texttt{\{}r\texttt{\}!}$ implies $w \models^{+} \texttt{\{}r\texttt{\}}$.

   It now suffices to show that $w \models^{+} \texttt{\{}r\texttt{\}}$ implies $w \models \texttt{\{}r\texttt{\}!}$. Assume $w \models^{+} \texttt{\{}r\texttt{\}}$. Then $w\bot^\omega \models \texttt{\{}r\texttt{\}}$. Since $|w\bot^\omega| > 0$, Lemma 8.5 implies that for every finite $u \preceq w\bot^\omega$, $u\top^\omega \models \texttt{\{}r\texttt{\}!}$ Since w is finite, we can take $u = w\bot$ to get

   $$w\bot\top^\omega \models \texttt{\{}r\texttt{\}!}$$

   so there exists $j \geq 0$ such that

   $$(w\bot\top^\omega)^{0..j} \models\!\models r$$

   By Lemma 7.2, $j < |w|$, so $w \models \texttt{\{}r\texttt{\}!}$.

□

Corollary 8.10. *Let w be a non-empty finite word over Σ, and let r be an unclocked* SERE*. The following are equivalent:*

- $w \models^{-} \texttt{\{}r\texttt{\}}$.
- $w \models^{-} \texttt{\{}r\texttt{\}!}$.
- $w \models \texttt{\{}r\texttt{\}}$.

□

Remark: The hypothesis that w be non-empty cannot be dropped from Corollary 8.10. If $|w| = 0$, then $w \models \texttt{\{}r\texttt{\}}$ holds vacuously for any unclocked SERE r. However, if

$$r = \texttt{\{[*0]\}} \;\texttt{\&\&}\; \texttt{\{}\text{TRUE}\texttt{\}}$$

then $w \not\models^{-} \texttt{\{}r\texttt{\}!}$. □

Lemma 8.11. *Let w be a finite word over Σ, let c be a boolean expression, and let r be a* SERE*.*

1. *The following are equivalent:*

   - $w \models^{c-} \texttt{\{}r\texttt{\}}$.
   - $w \models^{c-} \texttt{\{}r\texttt{\}!}$.
   - *For every finite $u \preceq w$, $u \models^{c-} \texttt{\{}r\texttt{\}!}$.*

2. *The following are equivalent:*

   - $w \models^{c+} \texttt{\{}r\texttt{\}}$
   - $w \models^{c+} \texttt{\{}r\texttt{\}!}$
   - $w \models^{c} \texttt{\{}r\texttt{\}!}$

Proof. Follows from Lemma 8.9 using Lemma 8.1 and Lemma 8.2. □

Corollary 8.12. *Let w be a non-empty finite word over Σ, let c be a boolean expression, and let r be a* SERE*. The following are equivalent:*

- $w \models^{c-} \texttt{\{}r\texttt{\}}$.
- $w \models^{c-} \texttt{\{}r\texttt{\}!}$.
- $w \models^{c} \texttt{\{}r\texttt{\}}$.

□

Remark: The hypothesis that w be non-empty cannot be dropped from Corollary 8.12. If $|w| = 0$, then $w \models^c$ `{r}` holds vacuously for any SERE r. However, if

$$r = \texttt{\{[*0]\}} \;\&\&\; \{\text{TRUE}\}$$

then $w \not\models^{c-}$ `{r}!`. □

Lemma 8.13. *Let w be a word over Σ, and let r be an unclocked* SERE.

1. $w \models$ `{r}!` *iff* $w \models^+$ `{r}!`.

2. *If* $w \models^-$ `{r}`, *then* $w \models$ `{r}`. *If* $|w| > 0$ *and* $w \models$ `{r}`, *then* $w \models^-$ `{r}`.

Proof. For w infinite, the results are immediate, since $w \models f$, $w \models^+ f$ and $w \models^- f$ are all equivalent. Assume w is finite. Part 1 follows from Lemma 8.9. By Lemma 8.7, $w \models$ `{r}` iff

$$|w| = 0 \text{ or for every finite } u \preceq w,\ u \models^- \texttt{\{r\}!}\ .$$

By Lemma 8.9, $w \models^-$ `{r}` iff

$$\text{for every finite } u \preceq w,\ u \models^- \texttt{\{r\}!}\ .$$

Hence Part 2. □

Lemma 8.14. *Let w be a word over Σ, let c be a boolean expression, and let r be a* SERE.

1. $w \models^c$ `{r}!` *iff* $w \models^{c+}$ `{r}!`.

2. *If* $w \models^{c-}$ `{r}`, *then* $w \models^c$ `{r}`. *If* $|w| > 0$ *and* $w \models^c$ `{r}`, *then* $w \models^{c-}$ `{r}`.

Proof. Follows from Lemma 8.13 using Lemma 8.1 and Lemma 8.2. □

9 Prefix/Extension theorem

This section proves that the Prefix/Extension Theorem of [4] holds for PSL, both in unclocked and clocked forms.

Theorem 9.1 (Unclocked Prefix/Extension). *Let u, v, w denote words over Σ, and let f be an unclocked PSL formula.*

1. $v \models^- f$ *iff for all* $u \preceq v$, $u \models^- f$.

2. $v \models^+ f$ *iff for all* $w \succeq v$, $w \models^+ f$.

Proof. Clearly the ($\Leftarrow$) direction holds in both cases. We prove the ($\Rightarrow$) direction by induction over the structure of f.

- $f = b!$.

  1. $v\top^\omega \models b!$
     iff $|v| = 0$ or $v^0 \Vdash b$
     $\Rightarrow$ for all $u \preceq v$, $|u| = 0$ or $u^0 \Vdash b$
     iff for all $u \preceq v$, $u\top^\omega \models b!$
  2. $v\bot^\omega \models b!$
     iff $|v| > 0$ and $v^0 \Vdash b$
     $\Rightarrow$ for all $w \succeq v$, $|w| > 0$ and $w^0 \Vdash b$
     iff for all $w \succeq v$, $w\bot^\omega \models b!$

- $f = (g)$.

  1. $v\top^\omega \models (g)$
     iff $v\top^\omega \models g$
     $\Rightarrow$ [induction]
     for all $u \preceq v$, $u\top^\omega \models g$
     iff for all $u \preceq v$, $u\top^\omega \models (g)$
  2. $v\bot^\omega \models (g)$
     iff $v\bot^\omega \models g$
     $\Rightarrow$ [induction]
     for all $w \succeq v$, $w\bot^\omega \models g$
     iff for all $w \succeq v$, $w\bot^\omega \models (g)$

- $f = !g$.

  1. $\neg$(for all $u \preceq v$, $u\top^\omega \models !g$)
     iff there exists $u \preceq v$ such that $\neg(u\top^\omega \models !g)$
     iff there exists $u \preceq v$ such that $\bar{u}\bot^\omega \models g$
     $\Rightarrow$ [induction]
     $\bar{v}\bot^\omega \models g$
     iff $\neg(v\top^\omega \models !g)$

2. $\neg$(for all $w \succeq v$, $w\bot^\omega \models \texttt{!}g$)
   iff there exists $w \succeq v$ such that $\neg(w\bot^\omega \models \texttt{!}g)$
   iff there exists $w \succeq v$ such that $\bar{w}\top^\omega \models g$
   $\Rightarrow$ [induction]
   $\bar{v}\top^\omega \models g$
   iff $\neg(v\bot^\omega \models \texttt{!}g)$

- $f = g \texttt{ \&\& } h$.

1. $v\top^\omega \models g \texttt{ \&\& } h$
   iff $v\top^\omega \models g$ and $v\top^\omega \models h$
   $\Rightarrow$ [induction]
   for all $u \preceq v$, $u\top^\omega \models g$ and $u\top^\omega \models h$
   iff for all $u \preceq v$, $u\top^\omega \models g \texttt{ \&\& } h$

2. $v\bot^\omega \models g \texttt{ \&\& } h$
   iff $v\bot^\omega \models g$ and $v\bot^\omega \models h$
   $\Rightarrow$ [induction]
   for all $w \succeq v$, $w\bot^\omega \models g$ and $w\bot^\omega \models h$
   iff for all $w \succeq v$, $w\bot^\omega \models g \texttt{ \&\& } h$

- $f = \texttt{\{}r\texttt{\}!}$.

1. Assume $v\top^\omega \models \texttt{\{}r\texttt{\}!}$. Then there exists $k \geq 0$ such that $(v\top^\omega)^{0..k} \models\!\!\models r$. If $u \preceq v$, then
$$(u\top^\omega)^{0..k} = (v^{0..|u|-1}\top^\omega)^{0..k}\ .$$
   By Lemma 7.4, $(u\top^\omega)^{0..k} \models\!\!\models r$, hence $u\top^\omega \models \texttt{\{}r\texttt{\}!}$.
2. Assume $v\bot^\omega \models \texttt{\{}r\texttt{\}!}$. Then there exists $k \geq 0$ such that $(v\bot^\omega)^{0..k} \models\!\!\models r$. By Lemma 7.2, $k < |v|$, hence $v^{0..k} \models\!\!\models r$. Therefore, if $w \succeq v$, then $(w\bot^\omega)^{0..k} = v^{0..k} \models\!\!\models r$, hence $w\bot^\omega \models \texttt{\{}r\texttt{\}!}$.

- $f = \texttt{\{}r\texttt{\}}$.

1. Assume $v\top^\omega \models \texttt{\{}r\texttt{\}}$. Let $u \preceq v$. If u is infinite, then v must be infinite, in which case
$$u\top^\omega = v\top^\omega \models \texttt{\{}r\texttt{\}}$$
   Otherwise, u is finite. Since $|v\top^\omega| > 0$, Lemma 8.5 gives $u\top^\omega \models \texttt{\{}r\texttt{\}!}$, so by Lemma 8.9, $u\top^\omega \models \texttt{\{}r\texttt{\}}$.
2. Assume $v\bot^\omega \models \texttt{\{}r\texttt{\}}$. Let $w \succeq v$. If v is infinite, then
$$w\bot^\omega = v\bot^\omega \models \texttt{\{}r\texttt{\}}$$
   Otherwise, v is finite. By Lemma 8.9, $v \models \texttt{\{}r\texttt{\}!}$, so there exists $0 \leq j < |v|$ such that $v^{0..j} \models\!\!\models r$. Since $v^{0..j} \preceq w\bot^\omega$, $w\bot^\omega \models \texttt{\{}r\texttt{\}!}$, and so by Lemma 8.7, $w\bot^\omega \models \texttt{\{}r\texttt{\}}$.

- $f = \texttt{X! } g$.

1. $v\top^\omega \models \texttt{X!}\ g$
   iff $(v\top^\omega)^{1..} \models g$
   iff $v^{1..}\top^\omega \models g$
   $\Rightarrow$ [induction; if $u \preceq v$, then $u^{1..} \preceq v^{1..}$]
   for all $u \preceq v$, $u^{1..}\top^\omega \models g$
   iff for all $u \preceq v$, $u\top^\omega \models \texttt{X!}\ g$
2. $v\bot^\omega \models \texttt{X!}\ g$
   iff $(v\bot^\omega)^{1..} \models g$
   iff $v^{1..}\bot^\omega \models g$
   $\Rightarrow$ [induction; if $w \succeq v$, then $w^{1..} \succeq v^{1..}$]
   for all $w \succeq v$, $w^{1..}\top^\omega \models g$
   iff for all $w \succeq v$, $w\top^\omega \models \texttt{X!}\ g$

- $f = \texttt{[}g\ \texttt{U}\ h\texttt{]}$.

1. $v\top^\omega \models \texttt{[}g\ \texttt{U}\ h\texttt{]}$
   iff there exists $k \geq 0$ such that $(v\top^\omega)^{k..} \models h$ and for all $0 \leq j < k$, $(v\top^\omega)^{j..} \models g$
   iff there exists $k \geq 0$ such that $v^{k..}\top^\omega \models h$ and for all $0 \leq j < k$, $v^{j..}\top^\omega \models g$
   $\Rightarrow$ [induction; $u \preceq v$ implies $u^{i..} \preceq v^{i..}$]
   for all $u \preceq v$, there exists $k \geq 0$ such that $u^{k..}\top^\omega \models h$ and for all $0 \leq j < k$, $u^{j..}\top^\omega \models g$
   iff for all $u \preceq v$, $u\top^\omega \models \texttt{[}g\ \texttt{U}\ h\texttt{]}$
2. $v\bot^\omega \models \texttt{[}g\ \texttt{U}\ h\texttt{]}$
   iff there exists $k \geq 0$ such that $(v\bot^\omega)^{k..} \models h$ and for all $0 \leq j < k$, $(v\bot^\omega)^{j..} \models g$
   iff there exists $k \geq 0$ such that $v^{k..}\bot^\omega \models h$ and for all $0 \leq j < k$, $v^{j..}\bot^\omega \models g$
   $\Rightarrow$ [induction; $w \succeq v$ implies $w^{i..} \succeq v^{i..}$]
   for all $w \succeq v$, there exists $k \geq 0$ such that $w^{k..}\top^\omega \models h$ and for all $0 \leq j < k$, $w^{j..}\top^\omega \models g$
   iff for all $w \succeq v$, $w\bot^\omega \models \texttt{[}g\ \texttt{U}\ h\texttt{]}$

- $f = g\ \texttt{abort}\ b$.

1. $v\top^\omega \models g\ \texttt{abort}\ b$
   iff $v\top^\omega \models g$ or there exists $k \geq 0$ such that $(v\top^\omega)^k \not\models b$ and $(v\top^\omega)^{0..k-1}\top^\omega \models g$
   iff $v\top^\omega \models g$ or there exists $k \geq 0$ such that $(v\top^\omega)^k \not\models b$ and $v^{0..k-1}\top^\omega \models g$
   $\Rightarrow$ [induction; if $u \preceq v$, then $u^{0..k-1} \preceq v^{0..k-1}$ and either $(u\top^\omega)^k = (v\top^\omega)^k$ or $(u\top^\omega)^k = \top$]
   for all $u \preceq v$, $u\top^\omega \models g$ or there exists $k \geq 0$ such that $(u\top^\omega)^k \not\models b$ and $u^{0..k-1}\top^\omega \models g$
   iff for all $u \preceq v$, $u\top^\omega \models g$ or there exists $k \geq 0$ such that $(u\top^\omega)^k \not\models b$ and $(u\top^\omega)^{0..k-1}\top^\omega \models g$
   iff for all $u \preceq v$, $u\top^\omega \models g\ \texttt{abort}\ b$
2. $v\bot^\omega \models g\ \texttt{abort}\ b$
   iff $v\bot^\omega \models g$ or there exists $k \geq 0$ such that $(v\bot^\omega)^k \not\models b$ and $(v\bot^\omega)^{0..k-1}\top^\omega \models g$

iff $v\top^\omega \models g$ or there exists $0 \le k < |v|$ such that $v^k \not\models b$ and $v^{0..k-1}\top^\omega \models g$
⇒ [induction; if $w \succeq v$, then $w^{0..k-1} \succeq v^{0..k-1}$ and if $0 \le k < |v|$, then $w^k = v^k$ and $w^{0..k-1} = v^{0..k-1}$]
for all $w \succeq v$, $w\bot^\omega \models g$ or there exists $0 \le k < |v|$ such that $w^k \not\models b$ and $w^{0..k-1}\top^\omega \models g$
iff for all $w \succeq v$, $w\bot^\omega \models g$ or there exists $0 \le k < |v|$ such that $(w\bot^\omega)^k \not\models b$ and $(w\bot^\omega)^{0..k-1}\top^\omega \models g$
⇒ for all $w \succeq v$, $w\bot^\omega \models g$ or there exists $k \ge 0$ such that $(w\bot^\omega)^k \not\models b$ and $(w\bot^\omega)^{0..k-1}\top^\omega \models g$
iff for all $w \succeq v$, $w\bot^\omega \models g$ `abort` b

- $f =$ `{`r`} |->` g.

1. First note that for any word w,

   $w\top^\omega \models$ `{`r`} |->` g
   iff for all $j \ge 0$ such that $(\bar{w}\bot^\omega)^{0..j} \models r$, $(w\top^\omega)^{j..} \models g$
   iff [Lemma 7.2]
   for all $0 \le j < |w|$ such that $\bar{w}^{0..j} \models r$, $w^{j..}\top^\omega \models g$

   Assume $v\top^\omega \models$ `{`r`} |->` g and let $u \preceq v$. Then for all $0 \le j < |v|$ such that $\bar{v}^{0..j} \models r$, $v^{j..}\top^\omega \models g$. It follows that for all $0 \le j < |u|$ such that $\bar{u}^{0..j} \models r$, $u^{j..}\top^\omega \models g$, and so $u\top^\omega \models$ `{`r`} |->` g.

2. Assume $v\bot^\omega \models$ `{`r`} |->` g and $w \succeq v$. Then for all $j \ge 0$ such that $(\bar{v}\top^\omega)^{0..j} \models r$, $v^{j..}\bot^\omega \models g$. Suppose $j \ge 0$ is such that $(\bar{w}\top^\omega)^{0..j} \models r$. Then by Lemma 7.4, it follows that $(\bar{v}\top^\omega)^{0..j} \models r$, and so $v^{j..}\bot^\omega \models g$. By induction, $w^{j..}\bot^\omega \models g$. This proves that $w\bot^\omega \models$ `{`r`} |->` g.

□

Theorem 9.2 (Clocked Prefix/Extension). *Let u, v, w denote words over Σ, let c be a boolean expression, and let f be an unclocked PSL formula.*

1. $v \models^{c-} f$ *iff for all* $u \preceq v$, $u \models^{c-} f$.

2. $v \models^{c+} f$ *iff for all* $w \succeq v$, $w \models^{c+} f$.

Proof. Follows from Theorem 9.1 using Corollary 5.4. □

10 Boolean formulas

This section discusses the promotion of boolean expressions to formulas and their relation to SERE formulas.

Lemma 10.1. *Let w be a word over Σ, and let b be a boolean expression.*

1. $w \models b!$ *iff* $w \models \{b\}!$ *iff* $w \models !(\{b\} \mid\!\!\rightarrow \text{FALSE})$.

2. $w \models b$ *iff* $w \models \{b\}$ *iff* $w \models \{!b\} \mid\!\!\rightarrow \text{FALSE}$.

Proof.

1. By Lemma 8.3, $w \models \{b\}!$ *iff* $w \models !(\{b\} \mid\!\!\rightarrow \text{FALSE})$.

   $w \models \{b\}!$
   iff there exists $0 \le j < |w|$ such that $w^{0..j} \not\models b$
   iff $[w^{0..j} \not\models b$ only if $j = 0]$
   $|w| > 0$ and $w^{0..0} \not\models b$
   iff $|w| > 0$ and $w^0 \not\models b$
   iff $w \models b!$

2. $w \models \{!b\} \mid\!\!\rightarrow \text{FALSE}$
   iff $\bar{w} \not\models !(\{!b\} \mid\!\!\rightarrow \text{FALSE})$
   iff [part 1]
   $\bar{w} \not\models \{!b\}!$
   iff $\neg(|\bar{w}| > 0$ and $\bar{w}^0 \not\models !b)$
   iff $|w| = 0$ or $\bar{w}^0 \not\models !b$
   iff [Lemma 3.5]
   $|w| = 0$ or $w^0 \not\models b$
   iff $w \models b$

   $w \models \{b\}$
   iff for all $0 \le j < |w|$, $w^{0..j}\top^\omega \models \{b\}!$
   iff for all $0 \le j < |w|$, there exists $0 \le k$ such that $(w^{0..j}\top^\omega)^{0..k} \not\models b$
   iff $[(w^{0..j}\top^\omega)^{0..k} \not\models b$ only if $k = 0]$
   for all $0 \le j < |w|$, $(w^{0..j}\top^\omega)^{0..0} \not\models b$
   iff $|w| = 0$ or $w^{0..0} \not\models b$
   iff $|w| = 0$ or ($|w| > 0$ and $w^0 \not\models b$)
   iff $|w| = 0$ or $w^0 \not\models b$
   iff $w \models b$

□

Lemma 10.2. *Let w be a word over Σ, and let b, c be boolean expressions. Then*

1. $w \models^c b!$ *iff* $w \models^c \{b\}!$ *iff* $w \models^c !(\{b\} \mid\!\!\rightarrow \text{FALSE})$.

2. $w \models^c b$ *iff* $w \models^c \{b\}$ *iff* $w \models^c \{!b\} \mid\!\!\rightarrow \text{FALSE}$.

Proof. By Lemma 8.3, $w \models^c$ `{`b`}!` *iff* $w \models^c$ `!({`b`} |->` FALSE`)`.

$w \models^c$ `{`b`}!`
iff there exists $0 \leq j < |w|$ such that $w^{0..j} \not\models^c b$
iff there exists $0 \leq j < |w|$ such that $w^{0..j}$ is a clock tick of c and $w^j \not\models b$
iff $w \models^c b$`!`

This proves 1.

$w \models^c$ `{!`b`} |->` FALSE
iff $\bar{w} \not\models^c$ `!({!`b`} |->` FALSE`)`
iff [part 1, Notation 3.6]
$\bar{w} \not\models^c$ `s(!`b`)`
iff $\neg$(there exists $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of c and $\bar{w}^j \not\models$ `!`b)
iff for all $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of c, $\bar{w}^j \not\not\models$ `!`b
iff [Lemma 3.5]
for all $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of c, $w^j \not\models b$
iff $w \models^c b$

Also

$w \models^c$ `{`b`}`
iff for all $0 \leq j < |w|$, $w^{0..j}\top^\omega \models^c$ `{`b`}!`
iff for all $0 \leq j < |w|$, there exists $0 \leq k$ such that $(w^{0..j}\top^\omega)^{0..k} \not\models^c b$
iff
(A):
for all $0 \leq j < |w|$, there exists $0 \leq k$ such that $(w^{0..j}\top^\omega)^{0..k}$ is a clock tick of c and $(w^{0..j}\top^\omega)^k \not\models b$

and

$w \models^c b$
iff
(B):
for all $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of c, $w^j \not\models b$

Assume (A). Let $0 \leq j < |w|$ be such that $\bar{w}^{0..j}$ is a clock tick of c. By (A), there exists $0 \leq k$ such that $(w^{0..j}\top^\omega)^{0..k}$ is a clock tick of c and $(w^{0..j}\top^\omega)^k \not\models b$. In order to prove (B), it suffices to show that $k = j$, since then it follows that $w^j = (w^{0..j}\top^\omega)^k \not\models b$. Suppose that $k < j$. Then $(w^{0..j}\top^\omega)^{0..k} = w^{0..k}$ is a clock tick of c, and so $w^k \not\models c$. Since $\bar{w}^{0..j}$ is a clock tick of c, $\bar{w}^k \not\models$ `!`c, so by Lemma 3.5, $w^k \not\not\models c$, a contradiction. Suppose that $k > j$. Then $(w^{0..j}\top^\omega)^{0..k} = w^{0..j}\top^{k-j}$ is a clock tick of c. Therefore, $w^j \not\models$ `!`c. Since $\bar{w}^{0..j}$ is a clock tick of c, $\bar{w}^j \not\models c$, so by Lemma 3.5, $w^j \not\not\models$ `!`c, a contradiction.

Now assume (B). Let

$$I = \{0 \leq i < |w| \colon w^i \notin 2^{\mathbf{P}} \text{ or } w^i \not\models c\} .$$

Suppose I is empty. Then, for all $0 \leq i < |w|$, $w^i \in 2^{\mathbf{P}}$ and $w^i \not\models$ `!`c. Let $0 \leq j < |w|$. Then $w^{0..j}\top$ is a clock tick of c and $(w^{0..j}\top)^{j+1} = \top \not\models b$. This proves (A) when I is empty. Suppose now that I is non-empty. Let $m = \min I$.

Then $m < |w|$ and for all $0 \leq i < m$, $w^i \in 2^{\mathbf{P}}$ and $w^i \Vdash\!\!\!= \, !c$. The following are the possible cases for w^m:

- $w^m = \bot$. Then $\bar{w}^{0..m}$ is a clock tick of c, so by (B) $w^m \Vdash\!\!\!= \, b$, a contradiction.
- $w^m = \top$. Then $w^{0..m}$ is a clock tick of c and $w^m \Vdash\!\!\!= \, b$.
- $w^m \in 2^{\mathbf{P}}$ and $w^m \Vdash\!\!\!= \, c$. Then $w^{0..m}$ is a clock tick of c and $\bar{w}^{0..m} = w^{0..m}$. By (B), $w^m \Vdash\!\!\!= \, b$.

Therefore, $w^{0..m}$ is a clock tick of c and $w^m \Vdash\!\!\!= \, b$. Let $0 \leq j < |w|$. If $j \geq m$, then $(w^{0..j}\top^\omega)^{0..m} = w^{0..m}$. If $j < m$, then $(w^{0..j}\top^\omega)^{0..j+1} = w^{0..j}\top$, which is a clock tick of c, and $(w^{0..j}\top^\omega)^{j+1} = \top \Vdash\!\!\!= \, b$. This proves (A) when I is non-empty and completes the proof of 2.

□

Lemma 10.3. *Let b, c be boolean expressions, and let w be a non-empty word over Σ such that $\bar{w}^0 \Vdash\!\!\!= \, c$. Then $w \models^c b$ iff $w \models^c b!$.*

Proof. Assume that $w \models^c b$. Since $\bar{w}^0 \Vdash\!\!\!= \, c$, $\bar{w}^{0..0}$ is a clock tick of c, hence $w^0 \Vdash\!\!\!= \, b$. Then $\bar{w}^0 \neq \bot$ and $w^0 \neq \bot$, hence $w^0 \in 2^{\mathbf{P}}$. Therefore, $w^{0..0}$ is a clock tick of c, and so $w \models^c b!$.

Assume now that $w \models^c b!$. Then there exists $0 \leq j < |w|$ such that $w^{0..j}$ is a clock tick of c and $w^j \Vdash\!\!\!= \, b$. Since $\bar{w}^0 \Vdash\!\!\!= \, c$, Lemma 3.5 gives $w^0 \not\Vdash\!\!\!= \, !c$. Therefore, $j = 0$ and so $w^0 \Vdash\!\!\!= \, c$ and $w^0 \Vdash\!\!\!= \, b$. Let $0 \leq i < |w|$ be such that $\bar{w}^{0..i}$ is a clock tick of c. Suppose that $0 < i$. Then $\bar{w}^0 \Vdash\!\!\!= \, !c$, so, by Lemma 3.5, $w^0 \not\Vdash\!\!\!= \, c$, a contradiction. Therefore $i = 0$. Since $w^0 \Vdash\!\!\!= \, b$, this proves that $w \models^c b$.

□

Lemma 10.4. *Let b, c be boolean expressions, and let w be a non-empty word over Σ.*

1. *If $w^0 = \top$, then $w \models^c b$ and $w \models^c b!$.*
2. *If $w^0 = \bot$, then $w \not\models^c b$ and $w \not\models^c b!$.*
3. *If $w^0 \in 2^{\mathbf{P}}$ and $w^0 \Vdash\!\!\!= \, c$, then $w \models^c b$ iff $w \models^c b!$ iff $w^0 \Vdash\!\!\!= \, b$.*

Proof. Assume $w^0 = \top$. Then $w^{0..0}$ is a clock tick of c and $w^0 \Vdash\!\!\!= \, b$, so $w \models^c b!$. Also, $\bar{w}^0 = \bot$, so there does not exist $0 \leq i < |w|$ such that $\bar{w}^{0..i}$ is a clock tick of c. Therefore, $w \models^c b$ holds vacuously. This proves 1.

Assume now that $w^0 = \bot$. Then there does not exist $0 \leq i < |w|$ such that $w^{0..i}$ is a clock tick of c, so $w \not\models^c b!$. Also, $\bar{w}^0 = \top$, so $\bar{w}^{0..0}$ is a clock tick of c. Since $w^0 \not\Vdash\!\!\!= \, b$, $w \not\models^c b$. This proves 2.

Assume now that $w^0 \in 2^{\mathbf{P}}$ and $w^0 \Vdash\!\!\!= \, c$. Then $w^0 = \bar{w}^0$, so by Lemma 10.3, $w \models^c b$ iff $w \models^c b!$.

$w \models^c b!$

iff there exists $0 \leq i < |w|$ such that $w^{0..i}$ is a clock tick of c and $w^i \not\models b$

iff [since $w^0 \in 2^{\mathbf{P}}$ and $w^0 \not\models c$, $w^{0..0}$ is a clock tick of c and $w^{0..i}$ is not a clock tick of c if $i > 0$]
$w^0 \not\models b$

This proves 3.

□

11 Semantics of formulas over proper words

This brief section shows that inductive definitions of the unclocked and clocked PSL formula satisfaction relations can be given for the set of proper words over Σ without relying on the definitions of formula satisfaction for non-proper words over Σ. Only minor changes to the definitions of unclocked and clocked satisfaction of a weak SERE formula are needed.

First note that if w is a proper word, then so are $\bar{w}$ and $w^{k\cdot\cdot}$ for any k. Also, if v is a word over $2^{\mathbf{P}}$, then vw is a proper word. Therefore, from Appendix B of [1], the only inductive references to formula satisfaction that require further scrutiny are in the definitions for the weak SERE form "$\{r\}$" and the abort form "f `abort` b". For each of these forms, the definition of satisfaction by a proper word w involves an inductive reference to satisfaction by words of the form $u\top^\omega$, where u is a finite prefix of w.

In the abort form, $u = w^{0..j-1}$ and the inductive reference to $w^{0..j-1}\top^\omega$ is guarded by $w^j \Vdash b$. Therefore w^j cannot be $\bot$, hence none of the letters of $w^{0..j-1}$ can be $\bot$, and so $w^{0..j-1}\top^\omega$ is proper.

In the weak SERE form, $u = w^{0..j}$ and the inductive reference is to $w^{0..j}\top^\omega \models \{r\}!$ in the unclocked case. In other words, the inductive reference requires that some non-empty prefix of $w^{0..j}\top^\omega$ tightly satisfy r. By Lemma 7.2, no word that tightly satisfies an unclocked SERE can have $\bot$ as a letter. If some letter of $w^{0..j}$ is $\bot$, then any non-empty prefix of $w^{0..j}\top^\omega$ that tightly satisfies r must be a prefix of $w^{0..j}$, hence also of $w^{0..j}\bot^\omega$. Therefore, the definition of unclocked satisfaction of a weak SERE formula can be changed to

$w \models \{r\}$
iff for all $0 \le j < |w|$, either
1. some letter of $w^{0..j}$ is $\bot$ and $w^{0..j}\bot^\omega \models \{r\}!$
or
2. no letter of $w^{0..j}$ is $\bot$ and $w^{0..j}\top^\omega \models \{r\}!$

Since w is proper, if some letter of $w^{0..j}$ is $\bot$, then $w^{0..j}\bot^\omega$ is proper, and if no letter of $w^{0..j}$ is $\bot$, then $w^{0..j}\top^\omega$ is proper.

Similar reasoning applies in the clocked case. The definition of clocked satisfaction of a weak SERE formula can be changed to

$w \models^c \{r\}$
iff for all $0 \le j < |w|$, either
1. some letter of $w^{0..j}$ is $\bot$ and $w^{0..j}\bot^\omega \models^c \{r\}!$
or
2. no letter of $w^{0..j}$ is $\bot$ and $w^{0..j}\top^\omega \models^c \{r\}!$

12 Miscellaneous lemmas on formulas

This section presents some miscellaneous lemmas on formulas, primarily from the work on mapping from SVA 3.1 to PSL 1.1.

Lemma 12.1. *Let f be a PSL formula, let c be a boolean expression, and let w be a proper word over Σ. Then the following are equivalent:*

1. $w \models^{\text{TRUE}}$ `(always` f`) @`c

2. *for all* $0 \leq i < |w|$ *such that* $\bar{w}^i \models c$, $w^{i..} \models^c f$

Proof.

$w \models^{\text{TRUE}}$ `(always` f`) @`c
iff $w \models^c$ `always` f
iff [Lemma 4.7]
for all $0 \leq k < |w|$ such that $\bar{w}^k \models c$, $w^{k..} \models^c f$

□

Lemma 12.2. *Let f be a PSL formula, let b and c be boolean expressions, and let w be a word over Σ. Then the following are equivalent:*

1. $w \models^c$ `(`b`! @`TRUE`) ->` f

2. *if* $|w| > 0$ *and* $\bar{w}^0 \models b$, *then* $w \models^c f$

If $|w| > 0$ *and* $\bar{w}^0 \models c$, *then 1 and 2 are equivalent to*

3. $w \models^c$ b`! ->` f

4. $w \models^c$ b `->` f

Proof.

$w \models^c$ `(`b`! @`TRUE`) ->` f
iff $w \models^c$ `!((`b`! @`TRUE`) && !`f`)`
iff $\bar{w} \not\models^c$ `(`b`! @`TRUE`) && !`f
iff $\bar{w} \not\models^c$ b`! @`TRUE or $\bar{w} \not\models^c$ `!`f
iff $\bar{w} \not\models^{\text{TRUE}}$ b`!` or $w \models^c f$
iff if $\bar{w} \models^{\text{TRUE}}$ b`!`, then $w \models^c f$
iff
(A):
if there exists $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of TRUE and
$\bar{w}^j \models b$, then $w \models^c f$

[(A) implies 2]: Assume (A). Assume $|w| > 0$ and $\bar{w}^0 \models b$. Then $\bar{w}^{0..0}$ is a clock tick of TRUE, so the precondition of (A) is satisfied with $j = 0$. Therefore $w \models^c f$.

[2 implies (A)]. Assume 2. Assume that there exists $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of TRUE and $\bar{w}^j \models b$. Then $|w| > 0$. If $j = 0$, then $\bar{w}^0 \models b$. If $j > 0$, then by Lemma 6.1, $\bar{w}^0 = \top$, hence $\bar{w}^0 \models b$. Therefore the precondition of 2 is satisfied, and so $w \models^c f$.

This proves that 1 and 2 are equivalent. Suppose now that $|w| > 0$ and $\bar{w}^0 \models c$.

$w \models^c b$ `->` f
iff $w \models^c$ `!((`b`!) && !`f`)`
iff $\bar{w} \not\models^c$ `(`b`!) && !`f
iff $\bar{w} \not\models^c b$`!` or $\bar{w} \not\models^c$ `!`f
iff $\bar{w} \not\models^c b$`!` or $w \models^c f$
iff if $\bar{w} \models^c b$`!`, then $w \models^c f$
iff
(B):
if (there exists $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of c and $\bar{w}^j \models b$), then $w \models^c f$

[(B) implies 2]: Assume (B). Assume $|w| > 0$ and $\bar{w}^0 \models b$. Since $\bar{w}^0 \models c$, $\bar{w}^{0..0}$ is a clock tick of c, so by (B), $w \models^c f$.

[2 implies (B)]. Assume 2. Suppose that $0 \leq j < |w|$ is such that $\bar{w}^{0..j}$ is a clock tick of c and $\bar{w}^j \models b$. Then $|w| > 0$. If $j = 0$, then $\bar{w}^0 \models b$. If $j > 0$, then $\bar{w}^0 \models$ `!`c. Since $\bar{w}^0 \models c$, $\bar{w}^0 = \top$, and so $\bar{w}^0 \models b$. Therefore the precondition of 2 is satisfied, and so $w \models^c f$.

This proves that 2 and 3 are equivalent if $|w| > 0$ and $\bar{w}^0 \models c$.

$w \models^c b$ `->` f
iff $w \models^c$ `!(`b `&& !`f`)`
iff $\bar{w} \not\models^c b$ `&& !`f
iff $\bar{w} \not\models^c b$ or $\bar{w} \not\models^c$ `!`f
iff $\bar{w} \not\models^c b$ or $w \models^c f$
iff [Lemma 10.4, using $|w| > 0$ and $\bar{w}^0 \models c$]
$\bar{w} \not\models^c b$`!` or $w \models^c f$
iff [proof of equivalence of 2 and 3]
(B)

Since (B) was shown equivalent to 2 when $|w| > 0$ and $\bar{w}^0 \models c$, this proves that 2 and 4 are equivalent when $|w| > 0$ and $\bar{w}^0 \models c$.

□

Lemma 12.3. *Let f be a PSL formula, let b and c be boolean expressions, and let w be a proper word over Σ. Then the following are equivalent:*

1. *for all $0 \leq j < |w|$ such that $\bar{w}^j \models c$ and $\bar{w}^j \models b$, $w^{j..} \models^c f$*

2. $w \models^{\text{TRUE}}$ `(always (`b`! ->` f`)) @`c

3. $w \models^{\text{TRUE}} \texttt{(always (}b \texttt{ -> } f\texttt{))} \texttt{@}c$

Proof.

$w \models^{\text{TRUE}} \texttt{(always (}b\texttt{! -> } f\texttt{))} \texttt{@}c$
iff [Lemma 12.1]
for all $0 \leq j < |w|$ such that $\bar{w}^j \Vdash c$, $w^{j\cdot\cdot} \models^c b\texttt{! -> } f$
iff [Lemma 12.2]
for all $0 \leq j < |w|$ such that $\bar{w}^j \Vdash c$, if $\bar{w}^j \Vdash b$, then $w^{j\cdot\cdot} \models^c f$
iff for all $0 \leq j < |w|$ such that $\bar{w}^j \Vdash c$ and $\bar{w}^j \Vdash b$, $w^{j\cdot\cdot} \models^c f$

This proves the equivalence of 1 and 2. A similar argument proves the equivalence of 1 and 3.

□

Acknowledgment: The work presented in this report was done as a result of the authors' participation in the Alignment Subcommittee of the Accellera Formal Verification Technical Committee (FVTC). We thank subcommittee members Roy Armoni and Johan Mårtensson for interesting discussions on some of the underlying issues.

References

[1] *Accellera Property Specification Language 1.1 Reference Manual*. Accellera Organization, Inc., Napa, California, 2004.

[2] *Accellera SystemVerilog 3.1 Language Reference Manual*. Accellera Organization, Inc., Napa, California, 2003.

[3] C. Eisner, D. Fisman, J. Havlicek. Weak regular expressions. Submitted for publication.

[4] C. Eisner, D. Fisman, J. Havlicek, Y. Lustig, A. McIsaac, D. Van Campenhout. Reasoning with temporal logic on truncated paths. In *Proc. 15th International Conference on Computer-Aided Verification (CAV)*, LNCS 2725, pp. 27–39. Springer, 2003.

[5] C. Eisner, D. Fisman, J. Havlicek, A. McIsaac, D. Van Campenhout. The definition of a temporal clock operator. In *Proc. 30th International Colloquium on Automata, Languages and Programming (ICALP)*, LNCS 2719, pp. 857–870. Springer, 2003.

[6] M. Gordon. PSL semantics in higher order logic. Available at `http://www.cl.cam.ac.uk/~mjcg/Talks/DCC04/paper.pdf`

A Appendix

For reference, the definitions from Appendix B of [1] of tight satisfaction of SEREs and of satisfaction of PSL formulas are copied here. The notations are adapted to the conventions of this report.

A.1 Semantics of unclocked SEREs

Let w, v_1, v_2 be finite words over Σ, let ℓ be a letter in Σ, let b be a boolean expression, and let r, r_1, r_2 be unclocked SEREs.

- $w \models \texttt{\{}r\texttt{\}}$ iff $w \models r$
- $w \models b$ iff $|w| = 1$ and $w^0 \Vdash b$
- $w \models r_1 \texttt{ ; } r_2$ iff there exist v_1, v_2 such that $w = v_1 v_2$, $v_1 \models r_1$, and $v_2 \models r_2$
- $w \models \texttt{\{}r_1\texttt{\} : \{}r_2\texttt{\}}$ iff there exist v_1, v_2, ℓ such that $w = v_1 \ell v_2$, $v_1 \ell \models r_1$, and $\ell v_2 \models r_2$
- $w \models \texttt{\{}r_1\texttt{\} || \{}r_2\texttt{\}}$ iff $w \models r_1$ or $w \models r_2$
- $w \models \texttt{\{}r_1\texttt{\} \&\& \{}r_2\texttt{\}}$ iff $w \models r_1$ and $w \models r_2$
- $w \models \texttt{[*0]}$ iff $|w| = 0$
- $w \models r\texttt{[*]}$ iff either $w \models \texttt{[*0]}$ or there exist v_1, v_2 such that $|v_1| > 0$, $w = v_1 v_2$, $v_1 \models r$, and $v_2 \models r\texttt{[*]}$

A.2 Semantics of unclocked formulas

Let w be a word over Σ, let b be a boolean expression, let r be an unclocked SERE, and let f, g be unclocked PSL formulas.

- $w \models \texttt{(}f\texttt{)}$ iff $w \models f$
- $w \models \texttt{!}f$ iff $\bar{w} \not\models f$
- $w \models f \texttt{ \&\& } g$ iff $w \models f$ and $w \models g$
- $w \models b\texttt{!}$ iff $|w| > 0$ and $w^0 \Vdash b$
- $w \models b$ iff $|w| = 0$ or $w^0 \Vdash b$
- $w \models \texttt{\{}r\texttt{\}!}$ iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models r$
- $w \models \texttt{\{}r\texttt{\}}$ iff for all $0 \leq j < |w|$, $w^{0..j}\top^\omega \models \texttt{\{}r\texttt{\}!}$
- $w \models \texttt{X! }f$ iff $|w| > 1$ and $w^{1..} \models f$
- $w \models \texttt{[}f \texttt{ U } g\texttt{]}$ iff there exists $0 \leq k < |w|$ such that $w^{k..} \models g$ and for all $0 \leq j < k$, $w^{j..} \models f$
- $w \models f \texttt{ abort } b$ iff either $w \models f$ or there exists $0 \leq j < |w|$ such that $w^j \Vdash b$ and $w^{0..j-1}\top^\omega \models f$
- $w \models \texttt{\{}r\texttt{\} |-> }f$ iff for all $0 \leq j < |w|$ such that $\bar{w}^{0..j} \models r$, $w^{j..} \models f$

A.3 Semantics of clocked SEREs

Let w, v_1, v_2 be finite words over Σ, let ℓ be a letter in Σ, let b, c, d be boolean expressions, and let r, r_1, r_2 be SEREs. w is a *clock tick* of c iff $|w| > 0$, $w^{|w|-1} \Vdash c$, and for all $0 \leq j < |w| - 1$, $w^j \Vdash \texttt{!}c$.

- $w \models^c \texttt{\{}r\texttt{\}}$ iff $w \models^c r$
- $w \models^c b$ iff w is a clock tick of c and $w^{|w|-1} \Vdash b$
- $w \models^c r_1 \texttt{ ; } r_2$ iff there exist v_1, v_2 such that $w = v_1 v_2$, $v_1 \models^c r_1$, and $v_2 \models^c r_2$
- $w \models^c \texttt{\{}r_1\texttt{\} : \{}r_2\texttt{\}}$ iff there exist v_1, v_2, ℓ such that $w = v_1 \ell v_2$, $v_1 \ell \models^c r_1$, and $\ell v_2 \models^c r_2$
- $w \models^c \texttt{\{}r_1\texttt{\} || \{}r_2\texttt{\}}$ iff $w \models^c r_1$ or $w \models^c r_2$
- $w \models^c \texttt{\{}r_1\texttt{\} \&\& \{}r_2\texttt{\}}$ iff $w \models^c r_1$ and $w \models^c r_2$
- $w \models^c \texttt{[*0]}$ iff $|w| = 0$
- $w \models^c r\texttt{[*]}$ iff either $w \models^c \texttt{[*0]}$ or there exist v_1, v_2 such that $|v_1| > 0$, $w = v_1 v_2$, $v_1 \models^c r$, and $v_2 \models^c r\texttt{[*]}$
- $w \models^c r \texttt{@}d$ iff $w \models^d r$

A.4 Semantics of clocked formulas

Let w be a word over Σ, let b, c, d be boolean expressions, let r be a SERE, and let f, g be PSL formulas.

- $w \models^c \texttt{(}f\texttt{)}$ iff $w \models^c f$
- $w \models^c \texttt{!}f$ iff $\bar{w} \not\models^c f$
- $w \models^c f \texttt{ \&\& } g$ iff $w \models^c f$ and $w \models^c g$
- $w \models^c b\texttt{!}$ iff there exists $0 \leq j < |w|$ such that $w^{0..j}$ is a clock tick of c and $w^j \Vdash b$
- $w \models^c b$ iff for all $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of c, $w^j \Vdash b$
- $w \models^c \texttt{\{}r\texttt{\}!}$ iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models^c r$
- $w \models^c \texttt{\{}r\texttt{\}}$ iff for all $0 \leq j < |w|$, $w^{0..j}\top^\omega \models^c \texttt{\{}r\texttt{\}!}$
- $w \models^c \texttt{X!}\ f$ iff there exist $0 \leq j < k < |w|$ such that $w^{0..j}$ and $w^{j+1..k}$ are clock ticks of c and $w^{k..} \models^c f$
- $w \models^c \texttt{[}f\texttt{ U }g\texttt{]}$ iff there exists $0 \leq k < |w|$ such that $w^k \Vdash c$, $w^{k..} \models^c g$, and for all $0 \leq j < k$ such that $\bar{w}^j \Vdash c$, $w^{j..} \models^c f$
- $w \models^c f \texttt{ abort } b$ iff either $w \models^c f$ or there exists $0 \leq j < |w|$ such that $w^j \Vdash b$ and $w^{0..j-1}\top^\omega \models^c f$
- $w \models^c \texttt{\{}r\texttt{\} |-> }f$ iff for all $0 \leq j < |w|$ such that $\bar{w}^{0..j} \models^c r$, $w^{j..} \models^c f$
- $w \models^c f \texttt{ @}d$ iff $w \models^d f$