Appendix D

Additional Proofs

In this appendix we provide the remaining proofs of chapter 4.

D.1 Properties of Metric M in Theorem 12

For the predicate transformer τ and the collection M of predicates defined by

$$\llbracket \tau.X \;\equiv\; q \vee \mathbf{wltr}\,.U.X \rrbracket$$
$$[M.0 \;\equiv\; \neg\,\mathbf{wltr}\,.U^{*}.q]$$
$$\langle \forall i : i > 0 : [M.i \;\equiv\; \tau^{i}.\,\text{false} \;\wedge\; \neg\langle \exists j : j < i : \tau^{j}.\,\text{false}\rangle]\rangle$$

we need to show the following:

$$[\langle \exists j : 0 < j \leq i : M.j\rangle \;\equiv\; \tau^{i}.\,\text{false}] \qquad \textbf{(M0)}$$
$$[\langle \exists i : i \in \mathbf{Ord} : M.i\rangle] \qquad \textbf{(M1)}$$
$$\langle \forall i, j : i \in \mathbf{Ord} \wedge j \in \mathbf{Ord} : i \neq j \Rightarrow [\neg M.i \vee \neg M.j]\rangle \qquad \textbf{(M2)}$$

(M1) and **(M2)** establish that M is a metric, **(M0)** is an auxiliary result used both in the proof of theorem 12 and in the proof of **(M1)**.

Proof . We first recall two properties of τ from section 4.2.1:

$$[\![\mathbf{wltr}.U^*.q \;\equiv\; \langle \exists i : i \in \mathbf{Ord} : \tau^i.\,\mathrm{false}\rangle]\!] \qquad \mathbf{(T2)}$$

$$\langle \forall i, j : i \le j : [\![\tau^i.\,\mathrm{false} \;\Rightarrow\; \tau^j.\,\mathrm{false}]\!]\rangle \qquad \mathbf{(T4)}$$

The proof of **(M0)** is by transfinite induction over i. For $i = 0$ the proof obligation is satisfied trivially. For any step ordinal i we observe

$$\begin{array}{ll}
 & \langle \exists j : 0 < j \le i : M.j\rangle \\
\equiv & \{\text{splitting the range, } i \text{ is step ordinal, induction hypothesis}\} \\
 & M.i \;\vee\; \tau^{i-1}.\,\mathrm{false} \\
\equiv & \{\text{definition of } M.i\} \\
 & (\tau^i.\,\mathrm{false} \;\wedge\; \neg\langle \exists j : j < i : \tau^j.\,\mathrm{false}\rangle) \;\vee\; \tau^{i-1}.\,\mathrm{false} \\
\equiv & \{\text{predicate calculus}\} \\
 & \tau^i.\,\mathrm{false} \;\vee\; \tau^{i-1}.\,\mathrm{false} \\
\equiv & \{\mathbf{(T4)}, \text{ predicate calculus}\} \\
 & \tau^i.\,\mathrm{false}
\end{array}$$

For any limit ordinal i we observe

$$\begin{array}{ll}
 & \langle \exists j : 0 < j \le i : M.j\rangle \\
\equiv & \{[M.i \equiv \mathrm{false}] \text{ since } i \text{ is limit ordinal}\} \\
 & \langle \exists j : 0 < j < i : M.j\rangle \\
\equiv & \{\text{predicate calculus}\} \\
 & \langle \exists k, j : 0 < j \le k < i : M.j\rangle \\
\equiv & \{\text{predicate calculus}\} \\
 & \langle \exists k : k < i : \langle \exists j : 0 < j \le k : M.j\rangle\rangle \\
\equiv & \{\text{induction hypothesis}\} \\
 & \langle \exists k : k < i : \tau^k.\,\mathrm{false}\rangle \\
\equiv & \{i \text{ is limit ordinal}\} \\
 & \tau^i.\,\mathrm{false}
\end{array}$$

For **(M1)** we observe

$$\begin{array}{ll}
 & \langle \exists i : i \in \mathbf{Ord} : M.i\rangle \\
\equiv & \{\text{splitting the range}\}
\end{array}$$

$$
\begin{array}{ll}
& M.0 \;\vee\; \langle \exists i : i > 0 : M.i \rangle \\
\equiv & \{\text{predicate calculus}\} \\
& M.0 \;\vee\; \langle \exists i, j : 0 < j \leq i : M.j \rangle \\
\equiv & \{\text{predicate calculus}\} \\
& M.0 \;\vee\; \langle \exists i : i \in \mathbf{Ord} : \langle \exists j : 0 < j \leq i : M.j \rangle \rangle \\
\equiv & \{\mathbf{(M0)}\} \\
& M.0 \;\vee\; \langle \exists i : i \in \mathbf{Ord} : \tau^i.\,\mathrm{false} \rangle \\
\equiv & \{\text{definition of } M.0,\ \mathbf{(T2)}\} \\
& \neg\, \mathbf{wltr}\,.U^*.q \;\vee\; \mathbf{wltr}\,.U^*.q \\
\equiv & \{\text{predicate calculus}\} \\
& \text{true}
\end{array}
$$

Finally, for **(M2)** we observe for any ordinal i with $i > 0$:

$$
\begin{array}{ll}
& M.i \wedge M.0 \\
\Rightarrow & \{\text{definition of } M.i, \text{ predicate calculus}\} \\
& \tau^i.\,\mathrm{false} \wedge M.0 \\
\Rightarrow & \{\text{definition of } M.0,\ \mathbf{(T2)}\} \\
& \mathbf{wltr}\,.U^*.q \;\wedge\; \neg\, \mathbf{wltr}\,.U^*.q \\
\equiv & \{\text{predicate calculus}\} \\
& \text{false}
\end{array}
$$

and for any ordinals i, j with $i > j$:

$$
\begin{array}{ll}
& M.i \wedge M.j \\
\Rightarrow & \{\text{definition of } M, \text{ predicate calculus}\} \\
& \neg \langle \exists k : k < i : \tau^k.\,\mathrm{false} \rangle \;\wedge\; \tau^j.\,\mathrm{false} \\
\Rightarrow & \{\text{predicate calculus, } i > j\} \\
& \neg \tau^j.\,\mathrm{false} \;\wedge\; \tau^j.\,\mathrm{false} \\
\equiv & \{\text{predicate calculus}\} \\
& \text{false}
\end{array}
$$

End of Proof.

D.2 Properties of Progress Algebras

In some of the following proofs of properties of progress algebras we use a small extension of the proof format introduced in section 2.1.3: when transforming algebraic expressions we allow $=$, $\leq$, and $\geq$ as operators relating subsequent lines of a proof in the same way as we use $\equiv$, $\Rightarrow$, and $\Leftarrow$ when relating lines of a proof consisting of transformations of logical expressions.

D.2.1 Proof of Lemma 15

Lemma 15 *In any left-handed or right-handed progress algebra $\mathcal{K}$, the subsumption relation $\leq$ defined by $U \leq V \;\equiv\; U+V = V$ is a partial order. Moreover the sequencing, alternation, and repetition operators are monotonic with respect to $\leq$, i.e., for all U, V, U' and V' in $\mathcal{K}$ with $U \leq V$ and $U' \leq V'$:*

$$UU' \;\leq\; VV' \qquad \textbf{\textit{(PrAlgSeq)}}$$

$$U+U' \;\leq\; V+V' \qquad \textbf{\textit{(PrAlgAlt)}}$$

$$U^* \;\leq\; V^* \qquad \textbf{\textit{(PrAlgStar)}}$$

Proof . Reflexivity, antisymmetry and transitivity of $\leq$ are easily shown using **(PrAlg0)** through **(PrAlg2)**[1]. Furthermore, we observe for all U, V, U' and V' in $\mathcal{K}$ with $U \leq V$ and $U' \leq V'$:

$$
\begin{array}{ll}
 & U+U' \;\leq\; V+V' \\
\equiv & \{\text{definition of } \leq\} \\
 & (U+U')+(V+V') \;=\; V+V' \\
\equiv & \{\textbf{(PrAlg0)}, \textbf{(PrAlg1)}\} \\
 & (U+V)+(U'+V') \;=\; V+V' \\
\equiv & \{U+V=V,\ U'+V'=V' \text{ from assumption}\} \\
 & \text{true}
\end{array}
$$

[1] This is an instance of the *Little Theory* in [DS90], stating that a relation $\leq$ defined in terms of a binary operator $+$ is reflexive if $+$ is idempotent, is antisymmetric if $+$ is commutative, and is transitive if $+$ is associative.

$$
\begin{array}{ll}
& UU' \ \leq \ VV' \\
\equiv & \{U + V = V,\ U' + V' = V' \text{ from assumption}\} \\
& UU' \ \leq \ (U + V)(U' + V') \\
\equiv & \{\textbf{(PrAlg7)}\} \\
& UU' \ \leq \ U(U' + V') + V(U' + V') \\
\Leftarrow & \{\textbf{(PrAlg6)},\ \textbf{(PrAlg0)}\} \\
& UU' \ \leq \ UU' + UV' + V(U' + V') \\
\equiv & \{\text{definition of } \leq\} \\
& UU' + (UU' + UV' + V(U' + V')) \ = \ UU' + UV' + V(U' + V') \\
\equiv & \{\textbf{(PrAlg0)},\ \textbf{(PrAlg2)}\} \\
& \text{true}
\end{array}
$$

For the * operator we first assume $\mathcal{K}$ to be right-handed. The case of $\mathcal{K}$ being left-handed is dealt with similarly.

$$
\begin{array}{ll}
& U^* \ \leq \ V^* \\
\Leftarrow & \{\text{transitivity of } \leq, \text{ preparing for } \textbf{(PrAlg11)}\} \\
& U^* \leq U^*V^* \ \wedge \ U^*V^* \leq V^* \\
\Leftarrow & \{\textbf{(PrAlgSeq)},\ \textbf{(PrAlg4)}\} \\
& \varepsilon \leq V^* \ \wedge \ U^*V^* \leq V^* \\
\equiv & \{\textbf{(PrAlg8)}, \text{ predicate calculus}\} \\
& U^*V^* \leq V^* \\
\Leftarrow & \{\textbf{(PrAlg11)}\} \\
& UV^* \leq V^* \\
\Leftarrow & \{\textbf{(PrAlg9)}\} \\
& UV^* \leq \varepsilon + VV^* \\
\equiv & \{\textbf{(PrAlg8)},\ \textbf{(PrAlg2)}; \text{ definition of } \leq,\ \textbf{(PrAlgAlt)}\} \\
& UV^* \leq VV^* \\
\Leftarrow & \{\textbf{(PrAlgSeq)}\} \\
& U \leq V \\
\equiv & \{\text{assumption}\} \\
& \text{true}
\end{array}
$$

End of Proof.

D.2.2 Proof of Lemma 16

Lemma 16 *In any left-handed or right-handed progress algebra $\mathcal{K}$, for all U, V, and W in $\mathcal{K}$ the following laws hold:*

$$\varepsilon + WW^* = W^* \qquad \textit{\textbf{(PrAlg13)}}$$

$$\varepsilon + W^*W = W^* \qquad \textit{\textbf{(PrAlg14)}}$$

$$W^*W^* = W^* \qquad \textit{\textbf{(PrAlg15)}}$$

$$(W^*)^* = W^* \qquad \textit{\textbf{(PrAlg16)}}$$

Furthermore, for right-handed $\mathcal{K}$ and all U, V, and W in $\mathcal{K}$:

$$V + UW \leq W \ \Rightarrow \ U^*V \leq W \qquad \textit{\textbf{(PrAlg17)}}$$

and for left-handed $\mathcal{K}$ and all U, V, and W in $\mathcal{K}$:

$$V + WU \leq W \ \Rightarrow \ VU^* \leq W \qquad \textit{\textbf{(PrAlg18)}}$$

Proof . One direction of **(PrAlg13)** and **(PrAlg14)** is given by **(PrAlg9)** and **(PrAlg10)**, respectively. The other direction follows easily from **(PrAlg8)**, **(PrAlgSeq)**, and the definition of $\leq$. For **(PrAlg15)** we observe for a right-handed progress algebra

$$
\begin{array}{ll}
 & W^*W^* \ \leq \ W^* \\
\Leftarrow & \{\textbf{(PrAlg11)}\} \\
 & WW^* \ \leq \ W^* \\
\equiv & \{\textbf{(PrAlg13)}\} \\
 & WW^* \ \leq \ \varepsilon + WW^* \\
\equiv & \{\textbf{(PrAlg2)}, \text{definition of } \leq\} \\
 & \text{true}
\end{array}
$$

and similarly for a left-handed progress algebra. We prove **(PrAlg16)** by mutual implication: for one direction we observe for a right-handed progress algebra

$$
\begin{aligned}
& (W^*)^* \ \leq \ W^* \\
\equiv \quad & \{\textbf{(PrAlg14)}\} \\
& \varepsilon + (W^*)^* W^* \ \leq \ W^* \\
\Leftarrow \quad & \{\textbf{(PrAlg2)}, \textbf{(PrAlgAlt)}, \textbf{(PrAlg8)}\} \\
& (W^*)^* W^* \ \leq \ W^* \\
\Leftarrow \quad & \{\textbf{(PrAlg11)}\} \\
& W^* W^* \ \leq \ W^* \\
\equiv \quad & \{\textbf{(PrAlg15)}\} \\
& \text{true}
\end{aligned}
$$

and similarly for a left-handed progress algebra. For the other direction we have

$$
\begin{aligned}
& W^* \ \leq \ (W^*)^* \\
\Leftarrow \quad & \{\textbf{(PrAlgStar)}\} \\
& W \ \leq \ W^* \\
\equiv \quad & \{\textbf{(PrAlg13)}\} \\
& W \ \leq \ \varepsilon + W W^* \\
\Leftarrow \quad & \{\textbf{(PrAlg8)}, \textbf{(PrAlgSeq)}, \textbf{(PrAlg2)}\} \\
& \text{true}
\end{aligned}
$$

Finally, we establish **(PrAlg17)** for a right-handed progress algebra; the proof of **(PrAlg18)** for a left-handed progress algebra is similar.

$$
\begin{aligned}
& V + UW \ \leq \ W \\
\Rightarrow \quad & \{\textbf{(PrAlg8)}, \textbf{(PrAlgAlt)}\} \\
& V \leq W \ \wedge \ UW \leq W \\
\Rightarrow \quad & \{\textbf{(PrAlg11)}\} \\
& V \leq W \ \wedge \ U^* W \leq W \\
\Rightarrow \quad & \{\textbf{(PrAlgSeq)}\} \\
& U^* V \leq W
\end{aligned}
$$

End of Proof.

D.2.3 Proof of Lemma 17

Lemma 17 *In any left-handed or right-handed progress algebra $\mathcal{K}$, for all $n \in \mathbf{N}$ with $n > 0$ and sequences W in $\mathbf{Z}_n \to \mathcal{K}$, for all permutations π of $\mathbf{Z}_n$, and for all U and V in $\mathcal{K}$ the following laws hold:*

$$UV \ \leq\ \varepsilon \quad\Rightarrow\quad U \ =\ \varepsilon \qquad \textbf{\textit{(PrAlg19)}}$$

$$UV \ \leq\ \varepsilon \quad\Rightarrow\quad V \ =\ \varepsilon \qquad \textbf{\textit{(PrAlg20)}}$$

$$U+V \ \leq\ \varepsilon \quad\Rightarrow\quad U \ =\ \varepsilon \qquad \textbf{\textit{(PrAlg21)}}$$

$$U^* \ \leq\ \varepsilon \quad\equiv\quad U \ =\ \varepsilon \qquad \textbf{\textit{(PrAlg22)}}$$

$$UU^* \ =\ U^* \qquad \textbf{\textit{(PrAlg23)}}$$

$$U^*U \ =\ U^* \qquad \textbf{\textit{(PrAlg24)}}$$

$$\langle +U : W : U\rangle \ \leq\ \langle \cdot U : W \circ \pi : U\rangle \qquad \textbf{\textit{(PrAlg25)}}$$

$$\langle +U : W : U\rangle^* \ =\ \langle \cdot U : W \circ \pi : U\rangle^* \qquad \textbf{\textit{(PrAlg26)}}$$

Proof . Due to **(PrAlg8)** it suffices to establish $\leq$ on the right-hand sides of **(PrAlg19)** through **(PrAlg22)**. For **(PrAlg19)** we observe

$$\begin{array}{ll} & U \\ = & \{\textbf{(PrAlg5)}\} \\ & U\varepsilon \\ \leq & \{\textbf{(PrAlg8)} \text{ for } V,\ \textbf{(PrAlgSeq)}\} \\ & UV \\ \leq & \{\text{antecedent}\} \\ & \varepsilon \end{array}$$

and similar for **(PrAlg20)**. For **(PrAlg21)** we observe

$$\begin{array}{ll} & U \\ \leq & \{\text{definition of } \leq,\ \textbf{(PrAlg2)}\} \\ & U+\varepsilon \\ \leq & \{\textbf{(PrAlg8)} \text{ for } V,\ \textbf{(PrAlgAlt)}\} \\ & U+V \end{array}$$

$$\leq \quad \{\text{antecedent}\}$$
$$\varepsilon$$

We prove **(PrAlg22)** by mutual implication:

$$U \leq \varepsilon$$
$$\Leftarrow \quad \{\text{transitivity of } \leq\}$$
$$U \leq U^*$$
$$\equiv \quad \{\textbf{(PrAlg13)}\}$$
$$U \leq \varepsilon + UU^*$$
$$\Leftarrow \quad \{\textbf{(PrAlg8)}, \textbf{(PrAlgSeq)}, \textbf{(PrAlg2)}\}$$
$$\text{true}$$

and, for a right-handed progress algebra (the proof for a left-handed progress algebra is similar),

$$\varepsilon^* \leq \varepsilon$$
$$\equiv \quad \{\textbf{(PrAlg5)}\}$$
$$\varepsilon^*\varepsilon \leq \varepsilon$$
$$\Leftarrow \quad \{\textbf{(PrAlg11)}\}$$
$$\varepsilon\varepsilon \leq \varepsilon$$
$$\equiv \quad \{\textbf{(PrAlg5)}\}$$
$$\text{true}$$

(PrAlg23) follows from **(PrAlg13)** and **(PrAlg8)**; similarly, **(PrAlg24)** follows from **(PrAlg14)** and **(PrAlg8)**.

As preparation for **(PrAlg25)** we note that for any U and V in $\mathcal{R}_F$, $U+V \leq UV$ holds by virtue of **(PrAlg8)**, **(PrAlgSeq)**, and **(PrAlg2)**.

We establish **(PrAlg25)** by induction over the length of W: the base case $|W| = 1$ is trivial; assuming that **(PrAlg25)** holds for all W of length n, we observe:

$$\langle +U : W : U \rangle$$
$$= \quad \{\textbf{(PrAlg0)},\textbf{(PrAlg1)}\}$$
$$\langle +U : W \circ \pi : U \rangle$$

$$
\begin{aligned}
&= \quad \{\text{quantification over sequences}\}\\
&\quad (W \circ \pi).0 \ + \ \langle +U : \mathbf{tail}.(W \circ \pi) : U \rangle\\
&\leq \quad \{\text{induction hypothesis}\}\\
&\quad (W \circ \pi).0 \ + \ \langle \cdot U : \mathbf{tail}.(W \circ \pi) : U \rangle\\
&\leq \quad \{\text{observation above}\}\\
&\quad (W \circ \pi).0 \ \cdot \ \langle \cdot U : \mathbf{tail}.(W \circ \pi) : U \rangle\\
&= \quad \{\text{quantification over sequences}\}\\
&\quad \langle \cdot U : W \circ \pi : U \rangle
\end{aligned}
$$

As preparation for **(PrAlg26)** we note that for any U in $\mathcal{R}_F$ and any natural n, $U^n \leq U^*$, where U^n denotes the sequence of n copies of U. This fact is proved by induction over n by virtue of **(PrAlg8)**, **(PrAlgSeq)**, and **(PrAlg23)**.

We establish **(PrAlg26)** by mutual implication. One direction follows from **(PrAlg25)** and **(PrAlgStar)**, the other is shown by induction over the length of W: the base case, $|W| = 1$, is trivial; assuming that **(PrAlg26)** holds for all W of length n, we observe

$$
\begin{aligned}
&\quad \langle \cdot U : W \circ \pi : U \rangle^*\\
&\leq \quad \{\textbf{(PrAlg8)}, \textbf{(PrAlgAlt)}, \textbf{(PrAlgSeq)}\}\\
&\quad \langle \cdot U : W \circ \pi : \langle +U : W : U \rangle \rangle^*\\
&= \quad \{\text{sequence calculus}\}\\
&\quad (\langle +U : W : U \rangle^n)^*\\
&\leq \quad \{\text{observation above}, \textbf{(PrAlgStar)}\}\\
&\quad (\langle +U : W : U \rangle^*)^*\\
&= \quad \{\textbf{(PrAlg16)}\}\\
&\quad \langle +U : W : U \rangle^*
\end{aligned}
$$

End of Proof.

D.2.4 Regular Languages with Subsumption as an Example of a Progress Algebra

In this section we show that the regular languages over an alphabet Σ are an instance of a progress algebra when ordered with respect to the subsumption relation introduced in section 2.1.6. In the following we call the algebraic structure $\mathcal{R}$ and denote for any W in $\mathcal{R}$ the language of W by $\mathcal{L}.W$.

First, we have to show that the subsumption order $\leq$ is consistent with the equality defined as $U = V \;\equiv\; U \leq V \;\wedge\; V \leq U$; i.e., we have to show that $U \leq V \;\equiv\; U + V = V$. This is done by observing that for any U and V in $\mathcal{R}$

$$
\begin{array}{ll}
 & \mathcal{L}.(U+V) \;=\; \mathcal{L}.V \\
\equiv & \{\text{definition of } \mathcal{L} \text{ and } =\} \\
 & ((\mathcal{L}.U \cup \mathcal{L}.V) \;\leq\; \mathcal{L}.V) \;\wedge\; (\mathcal{L}.V \;\leq\; (\mathcal{L}.U \cup \mathcal{L}.V)) \\
\equiv & \{\text{definition of } \leq, \text{ predicate calculus}\} \\
 & \mathcal{L}.U \;\leq\; \mathcal{L}.V
\end{array}
$$

Next, we have to show that all axioms of progress algebras are satisfied by $\mathcal{R}$. To this end, we establish a connection between $\mathcal{R}$ and the algebra of regular events $\mathbf{Reg}_\Sigma$. In the following we distinguish the equality in $\mathcal{R}$, written as $=$, from the equality on $\mathbf{Reg}_\Sigma$, which we write as $\equiv$, denoting the set-equality of the languages considered as sets of strings. It is obvious from the definitions of $=$, $\leq$, and $\equiv$, that for any U and V in $\mathcal{R}$, the following holds:

$$(\mathcal{L}.U \;\equiv\; \mathcal{L}.V) \quad\Rightarrow\quad (U \;=\; V)$$

This shows that all axioms, with the exception of **(PrAlg8)**, **(PrAlg11)**, and **(PrAlg12)**, are satisfied by $\mathcal{R}$ since they are satisfied by $\mathbf{Reg}_\Sigma$.

For any W in $\mathcal{R}$, $\mathcal{L}.\varepsilon \;\leq\; \mathcal{L}.W$ holds by virtue of the fact that the empty string is subsumed by any string, and that $\mathcal{L}.W$ is not empty. This shows that **(PrAlg8)** is satisfied.

Of the remaining **(PrAlg11)** and **(PrAlg12)** we show the first; the second is established similarly. We have to show that for any U and V in $\mathcal{R}$, $(\mathcal{L}.(UV) \leq \mathcal{L}.V) \Rightarrow (\mathcal{L}.(U^*V) \leq \mathcal{L}.V)$ holds. We observe

$$
\begin{array}{cl}
 & \mathcal{L}.(U^*V) \leq \mathcal{L}.V \\
= & \{\text{definition of } \mathcal{L}\} \\
 & (\langle \cup i : i \in \mathrm{N} : \mathcal{L}.U^i \rangle)(\mathcal{L}.V) \leq \mathcal{L}.V \\
\equiv & \{\text{set theory}\} \\
 & \langle \forall i : i \in \mathrm{N} : (\mathcal{L}.U^i)(\mathcal{L}.V) \leq \mathcal{L}.V \rangle
\end{array}
$$

which is easily established by induction over i using the antecedent $(\mathcal{L}.U)(\mathcal{L}.V) \leq \mathcal{L}.V$.

D.3 Soundness and Completeness of the Generalized Leads-To Relation

In this section we prove the soundness and completeness of the generalized leads-to relation with respect to the operational semantics given in section 4.5.2:

Theorem 21 (Soundness and Completeness) *For any program F and regular expression W in $\mathcal{R}_F$ the deductive system defined for generalized leads-to properties is sound and relatively complete in the sense of Cook:*

$$F \models \quad p \overset{W}{\longmapsto} q \qquad \textit{iff} \qquad F \vdash \quad p \overset{W}{\longmapsto} q$$

Using the definition of the operational semantic (definition 6) and theorem 12 we rewrite the proof obligation as follows: for any W in $\mathcal{R}_F$, and any p and q in $\mathcal{P}_F$

$$
\begin{array}{l}
\langle \exists w : w \in \mathcal{S}.W : \\
\qquad \langle \forall s, g : (s \models p \wedge \mathbf{si}.F) \wedge ((s,g) \ \mathbf{sat} \ w) : (s, \bar{g}) \models q \rangle\rangle \ \equiv \\
[p \Rightarrow \mathbf{wltr}.W.q]
\end{array}
$$

We prove soundness (implication from right-to-left) and completeness (implication from left-to-right) separately. First we introduce the notion of the *canonical strategy* $C.W.q$ for W and q in section D.3.1. After having established some auxiliary lemmata in section D.3.2, we then prove the soundness in section D.3.3 using canonical strategies by showing that

$$[p \Rightarrow \mathbf{wltr}.W.q] \;\Rightarrow$$
$$\langle \forall s, g : (s \models p \wedge \mathbf{si}.F) \wedge ((s,g)\ \mathbf{sat}\ C.W.q) : (s, \bar{g}) \models q \rangle.$$

Finally, in section D.3.4 we prove the completeness by establishing the contrapositive

$$\neg[p \Rightarrow \mathbf{wltr}.W.q] \;\Rightarrow$$
$$\langle \forall w : w \in \mathcal{S}.W : \langle \exists s, g : (s \models p \wedge \mathbf{si}.F) \wedge ((s,g)\ \mathbf{sat}\ w) : (s, \bar{g}) \not\models q \rangle\rangle.$$

D.3.1 Canonical Strategy

For a regular expression W in $\mathcal{R}_F$ and a goal predicate q in $\mathcal{P}_F$ we define the canonical strategy $C.W.q$ inductively over the structure of W as a specific element of $\mathcal{S}.W$ as follows. For all α in $F.A$ and all U, V in $\mathcal{R}_F$:

$$\begin{array}{lcl}
C.\varepsilon.q & = & \mathbf{eps} \\
C.\alpha.q & = & \mathbf{act}.\alpha \\
C.(UV).q & = & \mathbf{seq}.(C.U.(\mathbf{wltr}.V.q), C.V.q) \\
C.(U+V).q & = & \mathbf{alt}.(\mathbf{wltr}.U.q, C.U.q, C.V.q) \\
C.U^*.q & = & \mathbf{star}.(q, C.U.q)
\end{array}$$

From the proofs of the completeness theorem in section D.3.4 below we obtain the result that the canonical strategy is a *most general* strategy; i.e., if $F \models p \overset{W}{\longmapsto} q$ can be established with some strategy w in $\mathcal{S}.W$, then it can be established with $C.W.q$ as well.

D.3.2 Auxiliary Lemmata

Before we embark on the proofs of the soundness and completeness theorem we state and prove a few lemmata for later use. We start with a lemma that establishes a (conditional) stability result for $\mathbf{wltr}.W.q$ predicates:

Lemma 22 *For any α in $F.A$, q in $\mathcal{P}_F$, s in $F.S$, and W in $\mathcal{R}_F$:*

$$(s \models \neg q \wedge \mathbf{wltr}.W.q) \quad \Rightarrow \quad (\alpha.s \models \mathbf{wltr}.W.q)$$

Proof . The proof proceeds by induction on the structure of W. We observe for any U and V in $\mathcal{R}_F$ and any β in $F.A$:

case $W = \varepsilon$:

The antecedent is false due to **(wltrEps)**, hence the implication is satisfied trivially.

case $W = \beta$:

$$\begin{array}{ll} & s \models \neg q \wedge \mathbf{wltr}.\beta.q \\ \Rightarrow & \{\mathbf{(wltrAct)}\} \\ & s \models \neg q \wedge (q \vee (\mathbf{wco}.(q \vee \mathbf{wltr}.\beta.q) \wedge \mathbf{wp}.\beta.q)) \\ \Rightarrow & \{\text{predicate calculus}\} \\ & s \models \mathbf{wco}.(q \vee \mathbf{wltr}.\beta.q) \\ \Rightarrow & \{\text{definition of } \mathbf{wco}\text{, property of } \mathbf{wp}\text{, } \mathbf{(wltrWeaken)}\} \\ & \alpha.s \models \mathbf{wltr}.\beta.q \end{array}$$

case $W = UV$:

We consider two cases: for $s \not\models \mathbf{wltr}.V.q$ we observe

$$\begin{array}{ll} & s \models \neg q \wedge \mathbf{wltr}.(UV).q \\ \equiv & \{s \models \neg\,\mathbf{wltr}.V.q,\ \mathbf{(wltrWeaken)},\ \mathbf{(wltrSeq)}\} \\ & s \models \neg\,\mathbf{wltr}.V.q \ \wedge\ \mathbf{wltr}.U.(\mathbf{wltr}.V.q) \end{array}$$

$$\Rightarrow \quad \{\text{induction hypothesis for } U \text{ with } \mathbf{wltr}.V.q \text{ for } q, \ \mathbf{(wltrSeq)}\}$$
$$\alpha.s \models \mathbf{wltr}.(UV).q$$

If, on the other hand, $s \models \mathbf{wltr}.V.q$ holds, we observe

$$s \models \neg q \wedge \mathbf{wltr}.(UV).q$$
$$\equiv \quad \{s \models \mathbf{wltr}.V.q, \ \mathbf{(wltrSeq)}, \ \mathbf{(wltrWeaken)}\}$$
$$s \models \neg q \wedge \mathbf{wltr}.V.q$$
$$\Rightarrow \quad \{\text{induction hypothesis for } V\}$$
$$\alpha.s \models \mathbf{wltr}.V.q$$
$$\Rightarrow \quad \{\mathbf{(wltrWeaken)}, \ \mathbf{(wltrSeq)}\}$$
$$\alpha.s \models \mathbf{wltr}.(UV).q$$

case $W = U + V$:

$$s \models \neg q \wedge \mathbf{wltr}.(U+V).q$$
$$\equiv \quad \{\mathbf{(wltrAlt)}, \text{ definition of } \models, \text{ predicate calculus}\}$$
$$(s \models \neg q \wedge \mathbf{wltr}.U.q) \ \vee \ (s \models \neg q \wedge \mathbf{wltr}.V.q)$$
$$\Rightarrow \quad \{\text{induction hypothesis, twice}\}$$
$$(\alpha.s \models \mathbf{wltr}.U.q) \ \vee \ (\alpha.s \models \mathbf{wltr}.V.q)$$
$$\equiv \quad \{\text{definition of } \models, \ \mathbf{(wltrAlt)}\}$$
$$\alpha.s \models \mathbf{wltr}.(U+V).q$$

case $W = U^*$:

From $s \models \neg q \wedge \mathbf{wltr}.U^*.q$ we obtain by virtue of **(wltrStar)** that there is an ordinal i satisfying $s \models \neg q \wedge \tau^i.\text{false}$, where τ is defined by $[\![\tau.X \equiv q \vee \mathbf{wltr}.U.X]\!]$. We prove by induction over the ordinals that for all ordinals i

$$(s \models \neg q \wedge \tau^i.\text{false}) \ \Rightarrow \ (\alpha.s \models \tau^i.\text{false}) \ .$$

This assertion, together with the observation about the existence of a suitable ordinal and with with **(wltrStar)**, establishes the required result. For $i = 0$ and $i = 1$ the antecedent is false and the implication is satisfied trivially. If i is a limit ordinal, we have

$$
\begin{aligned}
& s \models \neg q \wedge \tau^i.\,\text{false} \\
\equiv \quad & \{i \text{ is limit ordinal}\} \\
& s \models \neg q \wedge \langle \exists l : l < i : \tau^l.\,\text{false}\rangle \\
\equiv \quad & \{\text{definition of } \models\text{, predicate calculus}\} \\
& \langle \exists l : l < i : s \models \neg q \wedge \tau^l.\,\text{false}\rangle \\
\Rightarrow \quad & \{\text{induction hypothesis for witness } l,\ \tau \text{ is monotonic}\} \\
& \alpha.s \models \tau^i.\,\text{false}
\end{aligned}
$$

If i is a step ordinal i greater than 1, we observe

$$
\begin{aligned}
& s \models \neg q \wedge \tau^i.\,\text{false} \\
\equiv \quad & \{\text{definition of } \tau,\ i \text{ is step ordinal, predicate calculus}\} \\
& s \models \neg q \wedge \mathbf{wltr}.U.(\tau^{i-1}.\,\text{false})
\end{aligned}
$$

Again, we consider two cases: for $s \not\models \tau^{i-1}.\,\text{false}$ we observe

$$
\begin{aligned}
& s \models \neg q \wedge \mathbf{wltr}.U.(\tau^{i-1}.\,\text{false}) \\
\equiv \quad & \{s \models \neg\tau^{i-1}.\,\text{false},\ [\![q \Rightarrow \tau^{i-1}.\,\text{false}]\!]\} \\
& s \models \neg\tau^{i-1}.\,\text{false} \wedge \mathbf{wltr}.U.(\tau^{i-1}.\,\text{false}) \\
\Rightarrow \quad & \{\text{induction hypothesis for } U \text{ with } \tau^{i-1}.\,\text{false for } q\} \\
& \alpha.s \models \mathbf{wltr}.U.(\tau^{i-1}.\,\text{false}) \\
\Rightarrow \quad & \{\text{definition of } \tau,\ \mathbf{(wltrStar)}\} \\
& \alpha.s \models \tau^i.\,\text{false}
\end{aligned}
$$

whereas for $s \models \tau^{i-1}.\,\text{false}$ we have

$$
\begin{aligned}
& s \models \neg q \wedge \mathbf{wltr}.U.(\tau^{i-1}.\,\text{false}) \\
\equiv \quad & \{s \models \tau^{i-1}.\,\text{false},\ \mathbf{(wltrWeaken)}\} \\
& s \models \neg q \wedge \tau^{i-1}.\,\text{false} \\
\Rightarrow \quad & \{\text{induction hypothesis for } i-1,\ \tau \text{ is monotonic}\} \\
& \alpha.s \models \tau^i.\,\text{false}
\end{aligned}
$$

End of Proof.

The intermediate assertion we established for the repetition case will be referred to later on; therefore, we restate it as a corollary as follows:

Corollary 23 *For any α in $F.A$, q in $\mathcal{P}_F$, s in $F.S$, W in $\mathcal{R}_F$, and ordinal i:*

$$(s \models \neg q \wedge \tau^i.\,\text{false}) \quad \Rightarrow \quad (\alpha.s \models \tau^i.\,\text{false}),$$

where τ is defined by $[\![\tau.X \equiv q \vee \mathbf{wltr}\,.W.X]\!]$.

The next lemma characterizes $\mathbf{wltr}\,.\alpha.q$ in terms of program executions:

Lemma 24 *For any α in $F.A$, q in $\mathcal{P}_F$, and s in $F.S$:*

$$\langle \forall x : x \in (F.A)^* : (s, x\alpha) \models q \rangle \quad \equiv \quad s \models \mathbf{wltr}\,.\alpha.q$$

Proof . The proof proceeds by mutual implication. Assuming $s \models \mathbf{wltr}\,.\alpha.q$, we define for any x consisting of k actions, $x.0$ through $x.(k-1)$, a sequence t of states as follows: $t.0 = s$, $t.(i+1) = (x.i).(t.i)$ for all i with $0 \leq i < k$, and $t.(k+1) = \alpha.(t.k)$. We show that there is an index i, $0 \leq i \leq k+1$, such that $t.i \models q$ by establishing that $\langle \forall i : i < k+1 : t.i \not\models q \rangle \ \Rightarrow \ (t.(k+1) \models q)$:

$$\begin{array}{ll} & \langle \forall i : i < k+1 : t.i \not\models q \rangle \\ \Rightarrow & \{t.0 \models \mathbf{wltr}\,.\alpha.q, \text{ lemma 22 } k\text{-times}\} \\ & t.k \models \neg q \wedge \mathbf{wltr}\,.\alpha.q \\ \Rightarrow & \{(\mathbf{wltrAct}), \text{ predicate calculus}\} \\ & t.k \models \mathbf{wp}\,.\alpha.q \\ \Rightarrow & \{\text{property of } \mathbf{wp}, \text{ definition of } t.(k+1)\} \\ & t.(k+1) \models q \end{array}$$

Conversely, we assume that $\langle \forall x : x \in (F.A)^* : (s, x\alpha) \models q \rangle$ holds. We define a predicate r by

$$(t \models r) \ \equiv \ \langle \forall x : x \in (F.A)^* : ((t, x) \not\models q) \ \Rightarrow \ (\alpha.(x.t) \models q) \rangle$$

Clearly, $s \models r$ holds. Next, we observe for all states t (the range for quantifications of x is understood to be $x \in (F.A)^*$):

$$
\begin{array}{ll}
& t \models r \\
\Rightarrow & \{\text{definition of } r\text{, predicate calculus}\} \\
& (t \models q) \;\vee\; ((t \not\models q) \wedge \langle \forall x :: ((t, x) \not\models q) \;\Rightarrow\; (\alpha.(x.t) \models q)\rangle) \\
\Rightarrow & \{\text{predicate calculus, instantiating } \langle\rangle \text{ and } x\beta \text{ for } x\} \\
& (t \models q) \;\vee\; ((\alpha.t \models q) \wedge \langle \forall \beta, x : \beta \in F.A : ((t, x\beta) \not\models q) \;\Rightarrow\; (\alpha.(x\beta.t) \models q)\rangle) \\
\equiv & \{\text{predicate calculus, definition of } r\} \\
& (t \models q) \;\vee\; ((\alpha.t \models q) \wedge \langle \forall \beta : \beta \in F.A : \beta.t \models r\rangle) \\
\equiv & \{\text{definition of } \mathbf{wco}\text{, property of } \mathbf{wp}\} \\
& (t \models q) \;\vee\; ((t \models \mathbf{wp}\,.\alpha.q) \wedge (t \models \mathbf{wco}\,.r)) \\
\Rightarrow & \{\mathbf{wco} \text{ is monotonic, predicate calculus, definition of } \models\} \\
& t \models q \vee (\mathbf{wco}\,.(r \vee q) \wedge \mathbf{wp}\,.\alpha.q)
\end{array}
$$

This establishes by virtue of **(wltrAct)** that r is a solution of the equation defining $\mathbf{wltr}\,.\alpha.q$. By the theorem of Knaster-Tarski we conclude that $[\![r \Rightarrow \mathbf{wltr}\,.\alpha.q]\!]$, which together with $s \models r$ establishes $s \models \mathbf{wltr}\,.\alpha.q$ as required.

End of Proof.

Lemma 25 *For any W and R in $\mathcal{R}_F$, such that R^* is a subexpression of W, and for any q in $\mathcal{P}_F$, there is an X in $\mathcal{R}_F$ such that the sub-strategy of $C.W.q$ corresponding to R^* has the form* $\mathbf{star}\,.(\mathbf{wltr}\,.X.q, R)$.

Proof . The required result follows from showing that for all W and R in $\mathcal{R}_F$ and all q and t in $\mathcal{P}_F$:

$$\mathbf{star}\,.(t, R) \text{ is a sub-strategy of } C.W.q \;\Rightarrow\; \langle \exists X : X \in \mathcal{R}_F : [\![t \equiv \mathbf{wltr}\,.X.q]\!] \rangle$$

This is proved by a straightforward induction over the structure of W, which is left as an exercise.

End of Proof.

D.3.3 Soundness

By virtue of the equivalence $[p] \;\equiv\; \langle \forall s : s \models \mathbf{si}.F : s \models p \rangle$ we can rephrase our proof obligation as follows:

$$\begin{array}{l} \langle \forall s : s \models p \wedge \mathbf{si}.F : \\ \qquad\qquad (s \models \mathbf{wltr}.W.q) \;\Rightarrow \langle \forall g : (s,g) \;\mathbf{sat}\; C.W.q : (s,\bar{g}) \models q \rangle \rangle. \end{array}$$

Proof . The proof proceeds by induction over the structure of W. We observe for all α in $F.A$, U and V in $\mathcal{R}_F$, p and q in $\mathcal{P}_F$, and s in $F.S$ satisfying $s \models p \wedge \mathbf{si}.F$:

case $W = \varepsilon$:

$$\begin{array}{ll} & (s,g) \;\mathbf{sat}\; C.\varepsilon.q \\ \equiv & \{\text{definition of } C.\varepsilon.q\text{, definition of } \mathbf{sat}\,\} \\ & g = \langle\rangle \end{array}$$

and, therefore,

$$\begin{array}{ll} & (s \models \mathbf{wltr}.\varepsilon.q) \;\Rightarrow\; \langle \forall g : (s,g) \;\mathbf{sat}\; C.\varepsilon.q : (s,\bar{g}) \models q \rangle \\ \equiv & \{\text{from above, } \mathbf{(wltrEps)}\} \\ & (s \models q) \;\Rightarrow\; ((s,\bar{\langle\rangle}) \models q) \\ \equiv & \{\text{predicate calculus}\} \\ & \text{true} \end{array}$$

case $W = \alpha$:

$$\begin{array}{ll} & (s,g) \;\mathbf{sat}\; C.\alpha.q \\ \equiv & \{\text{definition of } C.\alpha.q\text{, definition of } \mathbf{sat}\,\} \\ & \langle \exists x : x \in (F.A)^* : g = \langle x\alpha \rangle \rangle \end{array}$$

and, therefore,

$$\begin{array}{ll} & \langle \forall g : (s,g) \;\mathbf{sat}\; C.\alpha.q : (s,\bar{g}) \models q \rangle \\ \equiv & \{\text{from above, predicate calculus}\} \end{array}$$

$$\langle \forall x : x \in (F.A)^* : (s, x\alpha) \models q \rangle$$
$$\equiv \quad \{\text{lemma 24, antecedent, } s \models \mathbf{wltr}\,.\alpha.q\}$$
$$\text{true}$$

case $W = UV$:

For any game g for which $(s, g)\ \mathbf{sat}\ C.(UV).q$ holds, we obtain from the definitions of $C.(UV).q$ and **sat** that there exist games e and f satisfying the following conditions:

$$g = e +\!\!+ f \qquad \textbf{(SC0)}$$
$$(s, e)\ \mathbf{sat}\ C.U.(\mathbf{wltr}.V.q) \qquad \textbf{(SC1)}$$
$$\mathbf{finite}\,.\bar{e} \ \Rightarrow\ (\bar{e}.s, f)\ \mathbf{sat}\ C.V.q \qquad \textbf{(SC2)}$$

Assuming that $s \models \mathbf{wltr}\,.(UV).q$, we need to show that $(s, \bar{g}) \models q$. We do this by considering two cases depending on whether $\bar{e}$ is finite or infinite:

First we consider the case that $\mathbf{finite}\,.\bar{e}$ holds. Since $s \models \mathbf{wltr}\,.U.(\mathbf{wltr}\,.V.q)$ by **(wltrSeq)**, we have by virtue of **(SC1)** and the induction hypothesis for U (instantiating true for p and $\mathbf{wltr}\,.V.q$ for q):

$$(s, \bar{e}) \models \mathbf{wltr}\,.V.q \qquad \textbf{(SC3)}$$

If $(s, \bar{e}) \models q$ holds, we have $(s, \bar{g}) \models q$ because of **(SC0)**. Assuming $(s, \bar{e}) \not\models q$ we obtain from **(SC3)** that some state in the run $(s, \bar{e})$ satisfies $\neg q \wedge \mathbf{wltr}\,.V.q$. By repeated application of lemma 22 we obtain that $\bar{e}.s \models \mathbf{wltr}\,.V.q$. Together with **(SC2)** we have by virtue of the induction hypothesis for V (instantiating the reachable state $\bar{e}.s$ for s and true for p):

$$(\bar{e}.s, f) \models q$$

With the help of **(SC0)** we conclude $(s, \bar{g}) \models q$.

For the second case we assume $\bar{e}$ to be infinite. By **(SC1)**, e follows the strategy $C.U.(\mathbf{wltr}.V.q)$. There is only one way for $\bar{e}$ to be infinite: U contains a subexpression of the form R^*, the canonical sub-strategy corresponding to R^* is of the form $\mathbf{star}.(t, R)$ for some predicate t in $\mathcal{P}_F$, and from some point on e is made up from an infinite series of sub-games each of which follows the canonical strategy for R and ends in a state satisfying $\neg t$.

We define the infinite sequence E of runs by letting $E.i$ for natural i be the prefix of $\bar{e}$ up to the beginning of the R-sub-game number i (counting from 0). Since R is a subexpression of U, we have by lemma 25 that the sub-strategy for R has the form $\mathbf{star}.(\mathbf{wltr}.(XV).q, R)$ for some X in $\mathcal{R}_F$. As before, we have by virtue of **(SC1)** and the induction hypothesis for U:

$$(s, \bar{e}) \models \mathbf{wltr}.V.q$$

Let y be a prefix of $\bar{e}$ such that $y.s \models \mathbf{wltr}.V.q$ and let j be the smallest natural number for which y is a prefix of $E.j$. We show that $(s, E.j) \models q$: if this were not the case, we would have $y.s \models \neg q \wedge \mathbf{wltr}.V.q$. Repeated application of lemma 22 would establish $(E.j).s \models \mathbf{wltr}.V.q$, which together with **(wltrWeaken)** and **(wltrSeq)** would yield $(E.j).s \models \mathbf{wltr}.(XV).q$, contradicting the non-termination of e at the beginning of sub-game j. Hence, we have $(s, E.j) \models q$ and, by the definition of $E.j$ and by **(SC0)**, that $(s, \bar{g}) \models q$ holds as required.

case $W = U + V$:

Any game g, for which $(s, g)\ \mathbf{sat}\ C.(U+V).q$ holds, satisfies the following conditions by virtue of the definitions of $C.(U+V).q$ and **sat** :

$$(s \models \mathbf{wltr}.U.q) \ \Rightarrow \ ((s, g)\ \mathbf{sat}\ C.U.q) \qquad \mathbf{(SC4)}$$

$$(s \not\models \mathbf{wltr}.U.q) \ \Rightarrow \ ((s, g)\ \mathbf{sat}\ C.V.q) \qquad \mathbf{(SC5)}$$

We consider two cases depending on whether $\mathbf{wltr}.U.q$ holds in s or not: if $s \models$

$\mathbf{wltr}.U.q$, we obtain from **(SC4)** and the induction hypothesis for U that $(s, \bar{g}) \models q$. Similarly, if $s \not\models \mathbf{wltr}.U.q$, we obtain form the assumption $s \models \mathbf{wltr}.(U+V).q$, **(wltrAlt)**, **(SC5)** and the induction hypothesis for V that $(s, \bar{g}) \models q$.

case $W = U^*$:

From $s \models \mathbf{wltr}.U^*.q$ and **(wltrStar)** we conclude that there is a least ordinal l such that $s \models \tau^l.\text{false}$, where the predicate transformer τ is defined as $[\![\tau.X \equiv q \vee \mathbf{wltr}.U.X]\!]$.

In the following we define sequences k of ordinals, t of reachable states in $F.S$, e and f of games in $\mathcal{G}_F$, and E of finite runs in $(F.A)^*$. We define

$$
\begin{aligned}
k.0 &= l \\
t.0 &= s \\
f.0 &= g \\
E.0 &= \langle\rangle
\end{aligned}
$$

and maintain the following conditions for all natural numbers i, for which the respective elements are defined:

$$t.i \models \tau^{k.i}.\text{false} \quad \textbf{(SC6)}$$

$$(t.i, f.i)\ \mathbf{sat}\ C.U^*.q \quad \textbf{(SC7)}$$

$$E.i +\!\!+ \bar{f}.i = \bar{g} \quad \textbf{(SC8)}$$

$$t.i = (E.i).s \quad \textbf{(SC9)}$$

Clearly, all of these conditions are satisfied for $i = 0$ by virtue of the above definitions. We now describe the construction of later elements of the various sequences. The construction will establish $(s, \bar{g}) \models q$ eventually.

Following the definition of **sat** we consider two cases: if $t.i \models q$ holds then we have, by virtue of **(SC8)** and **(SC9)**, that $(s, \bar{g}) \models q$ and we are done.

We now assume $t.i \not\models q$. From the definition of **sat** we know that there exist games $e.i$ and $f.(i+1)$ satisfying the following conditions:

$$f.i = e.i +\!\!+ f.(i+1) \qquad \textbf{(SC10)}$$

$$(t.i, e.i) \ \textbf{sat}\ C.U.q \qquad \textbf{(SC11)}$$

$$\textbf{finite}\,.(\bar{e.i}) \ \Rightarrow \ ((\bar{e.i}).(t.i), f.(i+1)) \ \textbf{sat}\ C.U^*.q \qquad \textbf{(SC12)}$$

We, again, consider two cases depending on whether $\bar{e.i}$ is finite or infinite. For infinite $\bar{e.i}$ an argument similar to the one for the case of sequencing ($W = UV$) above establishes that $(t.i, \bar{e.i}) \models q$ and we are done by virtue of **(SC10)** and **(SC8)**.

For finite $\bar{e.i}$ we either have $(t.i, \bar{e.i}) \models q$ and we are done, or we have $(t.i, \bar{e.i}) \not\models q$. In this latter case we define $E.(i+1) = E.i +\!\!+ \bar{e.i}$ and define $t.(i+1)$ according to **(SC9)**. With this definition, **(SC8)** is maintained for $i+1$. **(SC12)** asserts **(SC7)** for $i+1$ as well. From **(SC6)** we conclude that $t.i \models \textbf{wltr}\,.U^*.q$; together with the fact that $(t.i, \bar{e.i}) \not\models q$ we obtain by repeated application of lemma 22 that $t.(i+1) \models \textbf{wltr}\,.U^*.q$ as well. Hence, there is a least ordinal $k.(i+1)$ for which $t.(i+1) \models \tau^{k.(i+1)}.\mathrm{false}$, thereby establishing **(SC6)** for $i+1$.

Next, we show that $k.(i+1) < k.i$. With this fact we see that, due to the well-foundedness of the ordinals, the above construction can be done only finitely many times and has to terminate with one of the cases establishing the goal $(s, \bar{g}) \models q$.

In order to establish that $k.(i+1) < k.i$, we summarize some properties of elements of our construction:

$$\textbf{finite}\,.(\bar{e.i}) \qquad \textbf{(SC13)}$$

$$(t.i, \bar{e.i}) \not\models q \qquad \textbf{(SC14)}$$

$$((\bar{e.i}).(t.i)) \models \tau^{k.(i+1)}.\mathrm{false} \qquad \textbf{(SC15)}$$

We prove that $k.(i+1) < k.i$ by induction over the ordinals. First, we note that $k.i > 0$ by **(SC6)**. Since $k.i$ is the least ordinal satisfying **(SC6)**, it is not a limit ordinal. Hence $k.i$ is a step ordinal. We observe by starting with **(SC6)**

$t.i \models \tau^{k.i}.\text{false}$

$\Rightarrow$ $\{k.i$ is step ordinal, definition of τ, **(SC14)**$\}$

$t.i \models \mathbf{wltr}.U.(\tau^{k.i-1}.\text{false})$

$\Rightarrow$ $\{$**(SC11)**, induction hypothesis for $U\}$

$(t.i, \bar{e.i}) \models \tau^{k.i-1}.\text{false}$

$\Rightarrow$ $\{$**(SC13)**, **(SC14)**, repeated application of corollary 23$\}$

$(\bar{e.i}).(t.i) \models \tau^{k.i-1}.\text{false}$

$\Rightarrow$ $\{$**(SC15)**, minimality of $k.(i+1)\}$

$k.(i+1) < k.i$

End of Proof.

D.3.4 Completeness

By virtue of the equivalence $[p] \equiv \langle \forall s : s \models \mathbf{si}.F : s \models p \rangle$ we can rephrase our proof obligation as follows:

$$\langle \exists s : s \models p \wedge \mathbf{si}.F : s \not\models \mathbf{wltr}.W.q \rangle \Rightarrow$$
$$\langle \forall w : w \in \mathcal{S}.W : \langle \exists s, g : (s \models p \wedge \mathbf{si}.F) \wedge ((s, g)\ \mathbf{sat}\ w) : (s, \bar{g}) \not\models q \rangle \rangle.$$

This proof obligation is discharged by showing that for any strategy w in $\mathcal{S}.W$, any s in $F.S$, and any q in $\mathcal{P}_F$:

$$(s \models \neg\, \mathbf{wltr}.W.q) \Rightarrow \langle \exists g : (s, g)\ \mathbf{sat}\ w : (s, \bar{g}) \not\models q \rangle$$

which we establish in the following for all W in $\mathcal{R}_F$.

Proof . The proof proceeds by induction over the structure of W. We observe for all q in $\mathcal{P}_F$, all α in $F.A$, and all U and V in $\mathcal{R}_F$:

case $W = \varepsilon$:

We choose $g = \langle\rangle$ which satisfies **eps**, the only strategy in $\mathcal{S}.\varepsilon$. We have

$$(s, \bar{g}) \not\models q$$

$$\equiv \quad \{g = \langle\rangle\}$$
$$(s \models \neg q)$$
$$\Leftarrow \quad \{\text{antecedent, } \mathbf{(wltrEps)}\}$$
$$\text{true}$$

case $W = \alpha$ for some $\alpha \in F.A$:

Careful inspection of the corresponding case in the soundness proof reveals that completeness has been established there as well (due to the equivalence in lemma 24).

case $W = UV$:

Any strategy w in $\mathcal{S}.W$ has the form $\mathbf{seq}.(u, v)$ for two strategies u in $\mathcal{S}.U$ and v in $\mathcal{S}.V$. Since $s \models \neg\,\mathbf{wltr}.U.(\mathbf{wltr}.V.q)$ by **(wltrSeq)**, there is by virtue of the induction hypothesis for U a game e satisfying (s, e) **sat** u, such that $(s, \bar{e}) \not\models \mathbf{wltr}.V.q$.

If $\bar{e}$ is infinite we have by **(wltrWeaken)** that $(s, \bar{e}) \not\models q$, and by the definition of **sat** that (s, e) **sat** w. Hence we choose $g = e$.

If $\bar{e}$ is finite, on the other hand, then from $(s, \bar{e}) \not\models \mathbf{wltr}.V.q$ it follows that $\bar{e}.s \models \neg\,\mathbf{wltr}.V.q$. By virtue of the induction hypothesis for V there is a game f satisfying $(\bar{e}.s, f)$ **sat** v, such that $(\bar{e}.s, \bar{f}) \not\models q$. We choose $g = e \mathbin{+\!\!+} f$ which satisfies both (s, g) **sat** w and $(s, \bar{g}) \not\models q$.

case $W = U + V$:

Any strategy w in $\mathcal{S}.W$ has the form $\mathbf{alt}.(t, u, v)$ for a predicate t and strategies u in $\mathcal{S}.U$ and v in $\mathcal{S}.V$. From the antecedent and from **(wltrAlt)** it follows that $s \models \neg\,\mathbf{wltr}.U.q \;\wedge\; \neg\,\mathbf{wltr}.V.q$. By virtue of the induction hypothesis for U, there is a game e with (s, e) **sat** u such that $(s, \bar{e}) \not\models q$. Similarly, there is a game f with

(s,f) **sat** v such that $(s,\bar{f}) \not\models q$. If $s \models t$ we choose $g = e$, otherwise we choose $g = f$.

case $W = U^*$:

We construct a game g for which $(s,\bar{g}) \not\models q$ holds as follows: starting with $f.0 = \langle\rangle$ we define games $f.i$ for natural i while maintaining the following two conditions:

$$(s, \bar{f.i}) \not\models q \qquad \textbf{(SC16)}$$

$$(\bar{f.i}).s \models \neg\,\mathbf{wltr}.U^*.q \qquad \textbf{(SC17)}$$

Since $s \models \neg\,\mathbf{wltr}.U^*.q$, both **(SC16)** and **(SC17)** are satisfied for $i = 0$. Any strategy w in $\mathcal{S}.W$ has the form $\mathbf{star}.(t,u)$ for a predicate t and a strategy u in $\mathcal{S}.U$. There are two possibilities for a game execution from state $(\bar{f.i}).s$ following strategy w: either $s \models t$, in which case the game terminates, or $s \not\models t$, in which case a game following strategy u is played. In the first case, we simply choose $g = f.i$, for which **(SC16)** establishes that $(s,\bar{g}) \not\models q$.

In the non-terminating case we have $(\bar{f.i}).s \models \neg\,\mathbf{wltr}.U.(\mathbf{wltr}.U^*.q)$, because $U^* = UU^*$ by **(PrAlg23)**. By virtue of the induction hypothesis for U, instantiating $\mathbf{wltr}.U^*.q$ for q, there exists a game e satisfying $((\bar{f.i}).s, e)$ **sat** u such that $((\bar{f.i}).s, e) \not\models \mathbf{wltr}.U^*.q$, which implies by virtue of **(wltrWeaken)** that $((\bar{f.i}).s, e) \not\models q$. We define $f.(i+1) = f.i \mathbin{+\!\!+} e$. Clearly, **(SC16)** is satisfied for $i+1$. If $\bar{e}$ is infinite we choose $g = f.(i+1)$ and are done. If $\bar{e}$ is finite we have from $((\bar{f.i}).s, e) \not\models \mathbf{wltr}.U^*.q$ that $\bar{e}.((\bar{f.i}).s) \models \neg\,\mathbf{wltr}.U^*.q$ establishing **(SC17)** for $i+1$. Hence we can repeat the construction until it terminates with one of the cases above, or we choose for g the limit of the $f.i$. In either case we have $(s,\bar{g}) \not\models q$ as required.

End of Proof.