Soundness Proof of Rule WF2

The proof uses the following tautologies, where F, G, and H are arbitrary temporal formulas.

T1. $\Box(F \Rightarrow G) \;\Rightarrow\; \Box(\Diamond F \Rightarrow \Diamond G)$

T2. $\Box(F \Rightarrow G) \;\Rightarrow\; \Box(\Box F \Rightarrow \Box G)$

T3. $\Box(F \Rightarrow G \lor H) \;\Rightarrow\; \Box(\Box F \Rightarrow \Box G \lor \Diamond H)$

T4. $\Box(F \land G \Rightarrow H) \;\Rightarrow\; \Box(\Box F \land \Box\Diamond G \Rightarrow \Box\Diamond H)$

Here is an informal proof of T1.

1. Suffices Assume: σ a behavior all of whose suffixes satisfy $F \Rightarrow G$, and τ a suffix of σ
   Prove: τ satisfies $\Diamond F \Rightarrow \Diamond G$
   Proof: By simple logic and definition of $\Box$.
2. It suffices to show that if ρ_1 is a suffix of τ satisfying F, then there is a suffix ρ_2 of τ satisfying G.
   Proof: By step 1 and the definitions of $\Diamond$ and $\Rightarrow$.
3. Q.E.D.
   Proof: By step 2, since ρ_1 is also a suffix of σ, so step 1 implies that we can take ρ_2 to equal ρ_1.

Proofs of T2–T4 are left to the reader. To save space in the proof of WF2, let's define

$$EB \;\triangleq\; \overline{\text{ENABLED } \langle B \rangle_w}$$

Here is the statement of WF2 written in the form $TR_{\Rightarrow}^{\Box}$ as an illegal temporal formula, and expressed for convenience as an assume/prove:

Assume: A1. $\Box(\langle \mathcal{N} \land C \rangle_v \Rightarrow \langle \overline{B} \rangle_{\overline{w}})$
A2. $\Box(P \land P' \land \langle \mathcal{N} \land A \rangle_v \land EB \Rightarrow C)$
A3. $\Box(P \land EB \Rightarrow \text{ENABLED } \langle A \rangle_v)$
A4. $\Box(\Box[\mathcal{N} \land \neg C]_v \land \mathrm{WF}_v(A) \land \Box EB \Rightarrow \Diamond\Box P)$
Prove: $\Box[\mathcal{N}]_v \land \mathrm{WF}_v(A) \;\Rightarrow\; \overline{\mathrm{WF}_w(B)}$

Here is its proof. Note that all the assumptions in assume clauses are $\Box$ formulas.

1. Suffices Assume: 1. $\Box[\mathcal{N}]_v$
   2. $\mathrm{WF}_v(A)$
   3. $\Diamond\Box EB$

PROVE: $\Diamond\langle\overline{B}\rangle_{\overline{w}}$

PROOF: Since $\overline{\mathrm{WF}_w(B)}$ is equivalent to $\Diamond\Box EB \Rightarrow \Box\Diamond\langle\overline{B}\rangle_{\overline{w}}$, it suffices to prove $\Box\Diamond\langle\overline{B}\rangle_{\overline{w}}$ under these assumptions. The result then follows from the rule $F \Vdash \Box F$.

2. $\Box[\mathcal{N} \land \neg C]_v \lor \Diamond\langle\mathcal{N} \land C\rangle_v$

2.1. $[\mathcal{N}]_v \Rightarrow [\mathcal{N} \land \neg C]_v \lor \langle\mathcal{N} \land C\rangle_v$

PROOF: This follows from the definitions of $[\ldots]_v$ and $\langle\ldots\rangle_v$ and the propositional logic tautology:

$$(U \lor V) \Rightarrow ((U \land \neg W) \lor V) \lor (U \land W \land \neg V)$$

2.2. Q.E.D.

By step 2.1, T3, and the rule $F \Vdash \Box F$.

3. $\Diamond\langle\mathcal{N} \land C\rangle_v \Rightarrow \Diamond\langle\overline{B}\rangle_{\overline{w}}$

PROOF: By T1 and assumption A1.

4. ASSUME: $\Box[\mathcal{N} \land \neg C]_v$

PROVE: $\Diamond\langle\overline{B}\rangle_{\overline{w}}$

4.1. $\Box[\mathcal{N} \land \neg C]_v \land \mathrm{WF}_v(A) \land \Diamond\Box EB \Rightarrow \Diamond\Box P$

PROOF: A4 and T1 imply

$$\Diamond\Box[\mathcal{N} \land \neg C]_v \land \Diamond\mathrm{WF}_v(A) \land \Diamond\Box EB \Rightarrow \Diamond\Diamond\Box P$$

Step 4.1 follows from this and the tautologies $F \Rightarrow \Diamond F$ and $\Diamond\Diamond F \equiv \Diamond F$.

4.2. $\Diamond\Box P$

PROOF: By 4.1, the steps 1 and 4 assumptions.

4.3. $\Diamond\Box\text{ENABLED }\langle A\rangle_v$

PROOF: From A3, using T1 and T2 and the tautology $\Diamond\Box(F \land G) \equiv \Diamond\Box F \land \Diamond\Box G$, we obtain

$$\Diamond\Box P \land \Diamond\Box EB \Rightarrow \Diamond\Box\text{ENABLED }\langle A\rangle_v$$

Step 4.3 follows from this, 4.2, and assumption 3 of step 1.

4.4. $\Box\Diamond\langle\mathcal{N} \land A\rangle_v$

PROOF: Step 4.3, assumption 2 of step 1, and the definition of WF imply $\Box\Diamond\langle A\rangle_v$. The result follows from this by T4 and assumption 1 of step 1, since $[N]_v \land \langle A\rangle_v$ implies $\langle\mathcal{N} \land A\rangle_v$.

4.5. $\Box\Diamond\langle\mathcal{N} \land C\rangle_v$

4.5.1. $\Box(P \land P' \land \langle\mathcal{N} \land A\rangle_v \land EB \Rightarrow \langle\mathcal{N} \land C\rangle_v)$

PROOF: By A2, since $\langle\mathcal{N} \land A\rangle_v \land C$ implies $\langle\mathcal{N} \land C\rangle_v$ by definition of $\langle\ldots\rangle_v$.

4.5.2. $\Diamond\Box(P \land P' \land EB) \land \Box\Diamond\langle\mathcal{N} \land A\rangle_v \Rightarrow \Box\Diamond\langle\mathcal{N} \land C\rangle_v$

PROOF: By 4.5.1 and T4

4.5.3. $\Diamond\Box(P \land P') \land \Diamond\Box EB \land \Box\Diamond\langle \mathcal{N} \land A \rangle_v \Rightarrow \Box\Diamond\langle \mathcal{N} \land C \rangle_v$

PROOF: By 4.5.2 and the tautology $\Diamond\Box(F \land G) \equiv \Box\Diamond F \land \Box\Diamond G$.

4.5.4. Q.E.D.

PROOF: By 4.2, 4.4, 4.5.3, assumption 3 of step 1, and the tautology $\Diamond\Box P \Rightarrow \Diamond\Box(P \land P')$.

5. Q.E.D.

PROOF: By steps 2, 3, and 4.