Appendix 1 to Lecture 26

J. Meseguer

Theorem 1. For each $\varphi \in LTL(\Pi)$ and pattern term u such that satisfaction of Π-predicates is defined in u, if $\mathcal{NK}(\mathcal{R}, State)_\Pi(u), u \models \varphi$, then $\forall \rho \in [vars(u) \to T_\Sigma],\ \ \mathcal{K}(\mathcal{R}, State)_\Pi, [u\rho] \models \varphi$.

Proof: Since $\mathcal{R}$ is deadlock-free, all paths from each ground instance $[u\rho]$ are non-terminating paths. Likewise, by the assumption that if $(l \to r) \in R$, then $l, r \in T_\Sigma(X)\backslash X$, the deadlock freedom of $\mathcal{R}$, and the Lifting Lemma for $\rightsquigarrow_{R,(E\cup B)}$, there are no finite, terminating narrowing paths from u in the narrowing tree of u, and, likewise, no such paths in $\mathcal{NK}(\mathcal{R}, State)_\Pi(u)$. We will be done if we prove that the set of *traces* associated to $\rightsquigarrow_\Pi$-narrowing paths from u in $\mathcal{NK}(\mathcal{R}, State)_\Pi(u)$ contains the set of all *traces* from $[u\rho]$ in $\mathcal{R}$ for all $\rho \in [vars(u) \to T_\Sigma]$. This follows from the following Lifting Lemma for $\rightsquigarrow_\Pi$.

Lemma (Lifting Lemma for $\rightsquigarrow_\Pi$). For any $v \in \mathcal{NK}(\mathcal{R}, State)_\Pi(u)$ and ground substitution ρ such that $[v\rho] \to_{R/E\cup B} [w]$, there is a $\rightsquigarrow_\Pi$-narrowing step $v \overset{\alpha\gamma}{\rightsquigarrow}_\Pi w'$ and a ground substitution τ such that $[w] = [w'\tau]$. Furthermore, v and $[v\rho]$ (resp. w' and $[w'\tau]$) satisfy the exact same predicates in Π.

Proof: By the Lifting Lemma for $\rightsquigarrow_{R,(E\cup B)}$, there is a narrowing step $v \overset{\alpha}{\rightsquigarrow}_{R,(E\cup B)} w'_0$ and a ground substitution τ_0 such that $[w'_0\tau_0] = [w]$. Let b_i be such that $[w] \models p_i = b_i$ for each $p_i \in \Pi$. Then, τ_0 is a $E \cup D \cup B$-unifier of the system of equations $\bigwedge_{p_i\in\Pi} w'_0 \models b_i$. Therefore, there must be a $E \cup D \cup B$-unifier γ and a ground substitution τ such that, $\gamma\tau =_{E\cup B} \tau_0$, so that for $w' =_{def} w'_0\gamma$, we have $v \overset{\alpha\gamma}{\rightsquigarrow}_\Pi w'$, and $[w'_0\gamma\tau] = [w'\tau] = [w]$, as desired. And, by construction, v and $[v\rho]$ (resp. w' and $[w'\tau]$) satisfy the exact same predicates in Π. □

Since we may assume without any loss of generality that in an infinite Π-narrowing path

$$(\dagger) \quad u \rightsquigarrow_\Pi u_1 \rightsquigarrow_\Pi u_2 \ldots u_n \rightsquigarrow_\Pi u_{n+1} \ldots$$

the variables of u_i and u_j with $i \neq j$ are *disjoint* (including $u_0 =_{def} u$), it follows easily from the Lifting Lemma for $\rightsquigarrow_\Pi$ that for any ground infinite path

$$(\ddagger) \quad [u\tau] \to_{R/E\cup B} [v_1] \to_{R/E\cup B} [v_2] \ldots [v_n] \to_{R/E\cup B} [v_{n+1}] \ldots$$

having a Π-narrowing path of the form (†) as its lifting, there is a ground substitution τ^e extending τ such that $[u_n\tau^e] = [v_n]$ for each $n \geqslant 1$. Therefore, all traces from ground instances of u are also traces of infinite Π-narrowing paths from u. This finishes the proof of the theorem. □

Theorem 2. If $f : \mathcal{A} \to \mathcal{B}$ is a Π-simulation (resp. Π-bisimulation) map of Kripke structures over Π, then, for any $a \in A$ and $\varphi \in LTL(\Pi)$,

$$\mathcal{B}, f(a) \models \varphi \ \Rightarrow\ (resp.\ \Leftrightarrow)\ \mathcal{A}, a \models \varphi.$$

Proof: Let us prove the ($\Rightarrow$) implication when $f : \mathcal{A} \to \mathcal{B}$ is a Π-simulation map. Each $\pi \in Path(\mathcal{A})_a$ yields a path $\pi; f \in Path(\mathcal{B})_{f(a)}$ having the exact same trace. Therefore, $\mathcal{B}, f(a) \models \varphi$ forces $\mathcal{A}, a \models \varphi$, as desired. Let us now prove the ($\Leftarrow$) implication when $f : \mathcal{A} \to \mathcal{B}$ is a Π-bisimulation map. Suppose this implication fails, so that $\mathcal{A}, a \models \varphi$ but $\mathcal{B}, f(a) \not\models \varphi$. This means that there is a path $\pi' \in Path(\mathcal{B})_{f(a)}$ such that $\pi' \not\models \varphi$. But, since f is a bisimulation map, there exists a path $\pi \in Path(\mathcal{A})_a$ with exact same trace as π' such that $\pi; f = \pi'$. But since $\mathcal{A}, a \models \varphi$ we must have $\pi' \models \varphi$, contradicting $\pi' \not\models \varphi$. $\square$

Theorem 3.

1. If $[\_]_{E \cup G \cup B}$ is a Π-simulation map, for each u and $\varphi \in LTL(\Pi)$,

$$FNG^{\Pi}_{\mathcal{R}/\mathcal{G}}(u), u \models \varphi \Rightarrow \mathcal{NK}(\mathcal{R}/\mathcal{G}, State)_{\Pi}(u), u \models \varphi \Rightarrow \mathcal{NK}(\mathcal{R}, State)_{\Pi}(u), u \models \varphi.$$

2. If $[\_]_{E \cup G \cup B}$ is a Π-bisimulation map, for each u and $\varphi \in LTL(\Pi)$,

$$FNG^{\Pi}_{\mathcal{R}/\mathcal{G}}(u), u \models \varphi \Rightarrow \mathcal{NK}(\mathcal{R}/\mathcal{G}, State)_{\Pi}(u), u \models \varphi \Leftrightarrow \mathcal{NK}(\mathcal{R}, State)_{\Pi}(u), u \models \varphi.$$

Furthermore, if φ a *safety formula*, the leftmost implication in (1) and (2) becomes an equivalence.

Proof: In both (1) and (2), the leftmost implication follows from Theorem 8 in Appendix 2; and for φ a safety formula, the leftmost equivalence follows from Theorem 12 in Appendix 2. The rightmost implication in (1) (resp. rightmost equivalence in (2)) follows form the fist part (resp. second part) of **Theorem** 2. $\square$