

Appendix 1 to Lecture 28

J. Meseguer

Theorem 1. For each $\varphi \in LTL(\Pi)$ and pattern disjunction $u_1 \vee \dots \vee u_n$ such that satisfaction of Π -predicates is defined for all u_i , $1 \leq i \leq n$, if $\mathcal{N}_{\mathcal{R}}^{\Pi}(u_1 \vee \dots \vee u_n), u_1 \vee \dots \vee u_n \models \varphi$, then $\forall \rho \in [vars(u_1 \vee \dots \vee u_n) \rightarrow T_{\Sigma}], \mathbb{T}_{\mathcal{R}}^{\Pi}, [u_i \rho] \models \varphi, 1 \leq i \leq n$.

Proof: Since \mathcal{R} is deadlock-free, all paths from each ground instance $[u_i \rho]$ are non-terminating paths. Likewise, by the assumption that if $(l \rightarrow r) \in R$, then $l, r \in T_{\Sigma}(X) \setminus X$, 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_i in the narrowing tree of u_i , and, likewise, no such paths in $\mathcal{N}_{\mathcal{R}}^{\Pi}(u_1 \vee \dots \vee u_n)$. We will be done if we prove that the set of *traces* associated to \rightsquigarrow_{Π} -narrowing paths from u in $\mathcal{N}_{\mathcal{R}}^{\Pi}(u_1 \vee \dots \vee u_n)$ contains the set of all *traces* from $[u_i \rho]$ in \mathcal{R} for all $\rho \in [vars(u_1 \vee \dots \vee u_n) \rightarrow T_{\Sigma}]$. This follows from the following Lifting Lemma for \rightsquigarrow_{Π} .

Lemma (Lifting Lemma for \rightsquigarrow_{Π}). For any $v \in \mathcal{N}_{\mathcal{R}}^{\Pi}(u_1 \vee \dots \vee u_n)$ and ground substitution ρ such that $[v\rho] \rightarrow_{R/E \cup B} [w]$, there is a \rightsquigarrow_{Π} -narrowing step $v \rightsquigarrow_{\Pi}^{\alpha\gamma} w'$ 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 $v \rightsquigarrow_{R, (E \cup B)}^{\alpha} w'_0$ 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 $v \rightsquigarrow_{\Pi}^{\alpha\gamma} w'$, 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 . \square

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

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

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_{Π} that for any ground infinite path

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

having a Π -narrowing path of the form (\dagger) as its lifting, there is a ground substitution τ^e extending τ such that $[u_n \tau^e] = [v_n]$ for each $n \geq 1$. 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. \square

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

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

Proof: Let us prove the (\Rightarrow) implication when $f : \mathcal{A} \rightarrow \mathcal{B}$ is a Π -simulation map. Each $\pi \in \text{Path}(\mathcal{A})_a$ yields a path $\pi; f \in \text{Path}(\mathcal{B})_{f(a)}$ 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 $f : \mathcal{A} \rightarrow \mathcal{B}$ 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 $\pi' \in \text{Path}(\mathcal{B})_{f(a)}$ such that $\pi' \not\models \varphi$. But, since f is a bisimulation map, there exists a path $\pi \in \text{Path}(\mathcal{A})_a$ 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 pattern disjunction $u_1 \vee \dots \vee u_n$ and $\varphi \in \text{LTL}(\Pi)$,

$$FNG_{\mathcal{R}/G}^{\Pi}(u_1 \vee \dots \vee u_n), u_1 \vee \dots \vee u_n \models \varphi \Rightarrow \mathcal{N}_{\mathcal{R}/G}^{\Pi}(u_1 \vee \dots \vee u_n), u_1 \vee \dots \vee u_n \models \varphi \Rightarrow \mathcal{N}_{\mathcal{R}}^{\Pi}(u_1 \vee \dots \vee u_n), u_1 \vee \dots \vee u_n \models \varphi.$$

2. If $[-]_{E \cup G \cup B}$ is a Π -bisimulation map, for each for each pattern disjunction $u_1 \vee \dots \vee u_n$ and $\varphi \in \text{LTL}(\Pi)$,

$$FNG_{\mathcal{R}/G}^{\Pi}(u_1 \vee \dots \vee u_n), u_1 \vee \dots \vee u_n \models \varphi \Rightarrow \mathcal{N}_{\mathcal{R}/G}^{\Pi}(u_1 \vee \dots \vee u_n), u_1 \vee \dots \vee u_n \models \varphi \Leftrightarrow \mathcal{N}_{\mathcal{R}}^{\Pi}(u_1 \vee \dots \vee u_n), u_1 \vee \dots \vee u_n \models \varphi.$$

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 from the first part (resp. second part) of **Theorem 2**. \square