Appendix to Lecture 26: Simulation Maps of Kripke Structures and Proofs of Theorems in Lecture 26

J. Meseguer

1 Simulation Maps between Kripke Structures

We can derive the theorems in Lecture 26 from considerably more general theorems about simulation maps between Kripke structures.

Definition 1. Given Kripke structures $\mathcal{K} = (K, \rightarrow_{\mathcal{K}}, \text{-}_{\mathcal{K}})$ and $\mathcal{Q} = (Q, \rightarrow_{\mathcal{Q}}, \text{-}_{\mathcal{Q}})$ over state predicate symbols Π, a Kripke structure *homomorphism*, also called a *simulation map* of Kripke structures, (resp. *strong homomorphism*, also called a *strong simulation map* of Kripke structures) from $\mathcal{K}$ to $\mathcal{Q}$, denoted $h : \mathcal{K} \rightarrow \mathcal{Q}$, is a function $h : K \rightarrow Q$ such that $\forall k, k' \in K$: (i) $k \rightarrow_{\mathcal{K}} k' \;\Rightarrow\; h(k) \rightarrow_{\mathcal{Q}} h(k'')$, and (ii) $\forall p \in \Pi$, $k \in p_{\mathcal{K}} \Rightarrow h(k) \in p_{\mathcal{Q}}$ (resp. (i) as above, and (ii)' $\forall p \in \Pi$, $k \in p_{\mathcal{K}} \Leftrightarrow h(k) \in p_{\mathcal{Q}}$). h is called injective, resp.surjective, resp. bijective, resp and isomorphism iff it is an injective, resp. surjective, resp. bijective function, resp. iff it is bijective and h^{-1} is also a simulation map. Note that h is an isomorphism iff it is bijective and $\forall k, k' \in K$: (i) $k \rightarrow_{\mathcal{K}} k' \;\Leftrightarrow\; h(k) \rightarrow_{\mathcal{Q}} h(k'')$, and (ii) $\forall p \in \Pi$, $k \in p_{\mathcal{K}} \Leftrightarrow h(k) \in p_{\mathcal{Q}}$. The expression *simulation map* is well-chosen, since $\mathcal{Q}$ can "simulate" any behaviors that $\mathcal{K}$ may perform and can do so in such a way that any predicate p satisfied by a state k of $\mathcal{K}$ is also satisfied by the state $h(k)$ simulating it in $\mathcal{Q}$ (for the strong case: and vice versa).

Theorem 1. For any simulation map of Kripke structures $h : \mathcal{K} \rightarrow \mathcal{Q}$ on Π, and state predicates $p_1, \ldots, p_n, p'_1, \ldots, p'_m \in \Pi$ the following implication holds:

$$\mathcal{R}, (p_1 \vee \ldots \vee p_n) \models_{S4} \Diamond(p'_1 \vee \ldots \vee p'_m) \quad \Rightarrow \quad \mathcal{Q}, (p_1 \vee \ldots \vee p_n) \models_{S4} \Diamond(p'_1 \vee \ldots \vee p'_m)$$

Proof: $\mathcal{R}, (p_1 \vee \ldots \vee p_n)_{\mathcal{K}} \models_{S4} \Diamond(p'_1 \vee \ldots \vee p'_m)_{\mathcal{K}}$ exactly means that there exist $k, k' \in K$, and i, j with $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$, such that $k \in p_{i_{\mathcal{K}}}$, $k' \in p'_{j_{\mathcal{K}}}$, and $k \rightarrow^*_{\mathcal{K}} k'$. But since h is a simulation map of Kripke structures, this forces $h(k) \in p_{i_{\mathcal{K}}}$, $k' \in p'_{j_{\mathcal{K}}}$, and $h(k) \rightarrow^*_{\mathcal{Q}} h(k')$, which exactly means that $\mathcal{Q}, (p_1 \vee \ldots \vee p_n)_{\mathcal{Q}} \models_{S4} \Diamond(p'_1 \vee \ldots \vee p'_m)_{\mathcal{Q}}$, as desired. $\square$

The notion of simulation map can be generalized to relate Kripke structures over different sets Π and Π' of state predicates by relating them by means of a fuction $H : \Pi \rightarrow \mathcal{P}_{fin}(\Pi')$, since H associates to each Π'-Kripke structure $\mathcal{Q} = (Q, \rightarrow_{\mathcal{Q}}, \text{-}_{\mathcal{Q}})$ the Π-Kripke structure $\mathcal{Q}|_H = (Q, \rightarrow_{\mathcal{Q}}, \text{-}_{\mathcal{Q}|_H})$, where for each $p \in \Pi$ with $H(p) = \{p'_1, \ldots, p'_n\}$, $p_{\mathcal{Q}|_H} = p'_{1\mathcal{Q}} \cup \ldots \cup p'_{n\mathcal{Q}}$.

Definition 2. Given Kripke structures $\mathcal{K}$ over Π and $\mathcal{Q}$ over Π', an H-*simulation map* of $\mathcal{K}$ by $\mathcal{Q}$ is by, definition, a simulation map $h : \mathcal{K} \rightarrow \mathcal{Q}|_H$. Note that a simulation map is the special case where of an H-simulation map where $\Pi = \Pi'$ and $H : \Pi \ni p \mapsto \{p\} \in \mathcal{P}_{fin}(\Pi)$. As an immediate corollary from **Theorem 1** and **Definition 2**, we obtain the following theorem for H-simulation maps:

Theorem 2. For any H-simulation map of Kripke structures $h : \mathcal{K} \to \mathcal{K}'$ on Π and Π', and state predicates $p_1, \ldots, p_n, p'_1, \ldots, p'_m \in \Pi$ with $H(p_i) = \{q_{i,j_1}, \ldots, q_{i,j_{r(i)}}\}$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant r(i)$, and $H(p'_{i'}) = \{q'_{i',j'_1}, \ldots, q'_{i',j'_{r'(i')}}\}$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant r'(i')$, the following implication holds:

$$\mathcal{K}, (p_1 \vee \ldots \vee p_n) \models_{S4} \Diamond(p'_1 \vee \ldots \vee p'_m) \;\; \Rightarrow \;\; \mathcal{K}', \bigvee_{1 \leqslant i \leqslant n} (q_{i,j_1} \vee \ldots \vee q_{i,j_{r(i)}}) \models_{S4} \Diamond \bigvee_{1 \leqslant i' \leqslant m} (q'_{i',j'_1} \vee \ldots \vee q'_{i',j'_{r'(i')}}).$$

The theorems in Lecture 26 either have a relatively easy proof, or follow as easy corollaries from the above two theorems.

2 Modal Logic Properties and Equational Abstractions

For ease of reference, the theorem in pg. 4 of Lecture 26 is here relabeled as **Proposition 1**.

Proposition 1. For $\mathcal{R}/G$ an equational abstraction of $\mathcal{R}$ and any state predicates $u_1, \ldots, u_n$, $v_1, \ldots, v_m \in T_\Sigma(X)_{State}$ the following holds:

$$\mathbb{T}_\mathcal{R}, (u_1 \vee \ldots \vee u_n) \models_{S4} \Diamond(v_1 \vee \ldots \vee v_m) \;\; \Rightarrow \;\; \mathbb{T}_{\mathcal{R}/G}, (u_1 \vee \ldots \vee u_n) \models_{S4} \Diamond(v_1 \vee \ldots \vee v_m)$$

Proof: By **Theorem 1**, all we need to prove is that the unique Σ-homomorphism

$$[\_]_{E \cup B \cup G} : \mathbb{T}_\mathcal{R} \to \mathbb{T}_{\mathcal{R}/G}$$

defines a simulation map of Kripke structures $[\_]_{E \cup B \cup G} : \mathbb{T}_\mathcal{R} = (T_{\Sigma/E \cup B, State}, \to_{R/E \cup B}, \text{-}_{\mathbb{T}_\mathcal{R}}) \to \mathbb{T}_{\mathcal{R}/G} = (T_{\Sigma/E \cup B \cup G, State}, \to_{R/E \cup B \cup G}, \text{-}_{\mathbb{T}_{\mathcal{R}/G}})$. This is trivially the case, since: (i) for any v, w ground terms of sort $State$, $u \to_{R/E \cup B} v \;\Rightarrow\; u \to_{R/E \cup B \cup G} v$, and (ii) for any $u T_\Sigma(X)_{State}$,

$$u_{\mathbb{T}_\mathcal{R}} = [\![u]\!]_{E \cup B} =_{def} \{[u\theta]_{E \cup B} \mid \theta \in [X \to T_\Sigma]\} \subseteq \{[u\theta]_{E \cup B \cup G} \mid \theta \in [X \to T_\Sigma]\} =_{def} [\![u]\!]_{E \cup B \cup G} = u_{\mathbb{T}_{\mathcal{R}/G}}. \;\square$$

For ease of reference, the theorem in pg. 10 of Lecture 26 is here relabeled as **Proposition 2**.

Proposition 2. Let φ'_i and call $u'_1 \mid \varphi'_1 \vee \ldots \vee u'_k \mid \varphi'_k$ be the *G-abstraction* of $u \mid \varphi$ in $\mathcal{R}/G$. The image of the set $[\![u \mid \varphi]\!]_{!_{\vec{E}/B}}$ under the unique surjective Σ-homomorphism:

$$[\_!_{\vec{E} \cup \vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}] : \mathbb{C}_{\Sigma/\vec{E},B} \to \mathbb{C}_{\Sigma/\vec{E},\vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}$$

is contained in the set $[\![(u'_1 \mid \varphi'_1 \vee \ldots \vee u'_k \mid \varphi'_k)]\!]_{!_{\vec{E} \cup \vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}}$.

Proof: We need to show that if $[v] \in [\![u \mid \varphi]\!]_{!_{\vec{E}/B}}$, then

$$[v!_{\vec{E} \cup \vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}] \in [\![(u'_1 \mid \varphi'_1 \vee \ldots \vee u'_k \mid \varphi'_k)]\!]_{!_{\vec{E} \cup \vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}}$$

But $[v] \in [\![u \mid \varphi]\!]_{!_{\vec{E}/B}}$ exactly means that $\exists \rho \in [X \to T_\Omega]$ *s.t.* $v =_B u\rho \;\wedge\; E \cup B \vdash \varphi\rho$. Abbreviate $u!_{\vec{E} \cup \vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}$ to u', and $\rho!_{\vec{E} \cup \vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}$ to τ. We then have $[v!_{\vec{E} \cup \vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}] = [u'\tau]$, and since $E \cup B \vdash \varphi\rho$ and φ is a conjunction of equalities, by the Church-Rosser Theorem a fortiori $E \cup \vec{E}'_{\Omega+} \cup B \cup B'_{\Omega+} \vdash \varphi\tau$. But since $u \mid \varphi$ has $u'_1 \mid \varphi'_1 \vee \ldots \vee u'_k \mid \varphi'_k$ as its

G-abstraction, this exactly means that there exists $1 \leqslant i \leqslant k$ and μ such that $\tau =_{B \cup B'_{\Omega+}} \gamma'_i \mu$ and $[v!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}] = [(u'\tau)!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}] = [u'_i \mu]$. But since we have

$$E \cup \vec{E'}_{\Omega+} \cup B \cup B'_{\Omega+} \vdash \varphi\tau \Leftrightarrow E \cup \vec{E'}_{\Omega+} \cup B \cup B'_{\Omega+} \vdash \varphi'_i \mu$$

we then have $[v!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}] \in [\![(u'_1 \mid \varphi'_1 \vee \ldots \vee u'_k \mid \varphi'_k)]\!]_{!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}}$, as desired. $\square$

For ease of reference, the theorem in pg. 12 of Lecture 26 is here relabeled as **Proposition 3**.

Proposition 3. If all rules in the topmost theory $\mathcal{R}$ are G-abstractable, $\widehat{\mathcal{R}/G}$ is admissible.

Proof: By the assumptions on $\mathcal{R}$ and G, all we need to prove to show that $\widehat{\mathcal{R}/G}$ is admissible is that the rules $\widehat{R}$ in $\widehat{\mathcal{R}/G}$ are ground coherent with the oriented equations $\vec{E} \cup \vec{E'}_{\Omega+}$ modulo $B \cup B'_{\Omega+}$. Let t be a ground term such that $t \rightarrow_{\widehat{R}/B \cup B'_{\Omega+}} t'$. Since any rule in $\widehat{R}$ is of the form $l'_i \rightarrow r'_i \;\; \textit{if} \;\; \varphi'_i$ in some G-abstraction $\{l'_i \rightarrow r'_i \;\; \textit{if} \;\; \varphi'_i\}_{1 \leqslant i \leqslant k}$ of some rule $l \rightarrow r \;\; \textit{if} \;\; \varphi$ in $\mathcal{R}$, there exists a rule $l'_i \rightarrow r'_i \;\; \textit{if} \;\; \varphi'_i$ of this form and a ground substitution θ such that $t =_{B \cup B'_{\Omega+}} l'_i \theta$, $t' =_{B \cup B'_{\Omega+}} r'_i \theta$, and $E \cup E'_{\Omega+} \cup B \cup B'_{\Omega+} \vdash \varphi'_i \theta$. But since $l'_i =_{def} (l\gamma_i)!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}$, if $\vec{y} = \textit{vars}(l\gamma_i) \backslash \textit{vars}(l'_i)$ we can choose any ground substitution τ of the variables $\vec{y}$ so that $E \cup E'_{\Omega+} \cup B \cup B'_{\Omega+} \vdash \varphi\gamma_i(\theta \uplus \tau)$. Let $u = t!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}$. We will be done if we show a rewrite step $u \rightarrow_{\widehat{R}/B \cup B'_{\Omega+}} u'$ such that $u'!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} =_{B \cup B'_{\Omega+}} t'!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}$. But $u = t!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} =_{B \cup B'_{\Omega+}} (l_i\theta)!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} =_{B \cup B'_{\Omega+}} (l(\gamma_i(\theta \uplus \tau)))!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}$. Therefore, there exists a rule $l'_j \rightarrow r'_j \;\; \textit{if} \;\; \varphi'_j$ in the abstraction of $l \rightarrow r \;\; \textit{if} \;\; \varphi$ and a $\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}$-normalized substitution μ such that $u =_{B \cup B'_{\Omega+}} l'_j \mu$, with $\gamma_j \mu =_{B \cup B'_{\Omega+}} (\gamma_i(\theta \uplus \tau))!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}$. Let $u' = r_j \mu$. Since, furthermore, $E \cup E'_{\Omega+} \cup B \cup B'_{\Omega+} \vdash \varphi'_i \mu$ holds. because $E \cup E'_{\Omega+} \cup B \cup B'_{\Omega+} \vdash \varphi\gamma_i(\theta \uplus \tau)$ does and $\gamma_j \mu =_{B \cup B'_{\Omega+}} (\gamma_i(\theta \uplus \tau))!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}$, we indeed have a rewrite step $u \rightarrow_{\widehat{R}/B \cup B'_{\Omega+}} u'$ that satisfies $u'!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} =_{B \cup B'_{\Omega+}} t'!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}$ as desired, because $u'!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} = (r_j\mu)!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} =_{B \cup B'_{\Omega+}} (r(\gamma_i(\theta \uplus \tau)))!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} =_{B \cup B'_{\Omega+}} (r_i\theta)!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} = t'!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}$. $\square$

Proposition 3 has the following important corollary:

Corollary 1. Under the assumptions of **Proposition 3**, If $[u] \rightarrow_{\mathcal{R}} [v]$ in $\mathbb{C}_{\mathcal{R}}$, then $[u!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}] \rightarrow_{\mathcal{R}} [v!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}]$ in $\mathbb{C}_{\widehat{\mathcal{R}/G}}$.

Proof: By definition, $[u] \rightarrow_{\mathcal{R}} [v]$ means that there is a rule $l \rightarrow r \;\; \textit{if} \;\; \varphi$ in $\mathcal{R}$ and a ground substitution ρ such that $[u] = l\rho$, $[v] = [r\rho!_{\vec{E}/B}]$, and $E \cup B \vdash \varphi\rho$. But then $u!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} =_{B \cup B'_{\Omega+}} (l\rho)!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}$. Therefore, there is a rule $l'_i \rightarrow r'_i \;\; \textit{if} \;\; \varphi'_i$ in the G-abstraction of $l \rightarrow r \;\; \textit{if} \;\; \varphi$ and a ground substitution τ such that $(l\rho)!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} =_{B \cup B'_{\Omega+}} l_i\tau$, $(r\rho)!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} =_{B \cup B'_{\Omega+}} r_i\tau$, and $(\rho)!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} =_{B \cup B'_{\Omega+}} \gamma_i\tau$. Furthermore, $E \cup E'_{\Omega+} \cup B \cup B'_{\Omega+} \vdash \varphi'_i \tau$ holds because this is equivalent to $E \cup E'_{\Omega+} \cup B \cup B'_{\Omega+} \vdash \varphi\gamma_i\tau$, which is forced by $E \cup B \vdash \varphi\rho$ since $(\rho)!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}} =_{B \cup B'_{\Omega+}} \gamma_i\tau$. Therefore, $[u!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}] \rightarrow_{\mathcal{R}} [v!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}]$, as desired. $\square$

For ease of reference, the Main Theorem for explicit-state model checking in pg. 17 of Lecture 26 is here relabeled as **Proposition 4**.

Proposition 4. (Explicit-State Model Checking with Equational Abstractions). For $\mathcal{R}$ topmost and admissible with all its rules G-abstractable and $(v_1 \mid \varphi_1 \vee \ldots \vee v_m \mid \varphi_m)$ such that each $v_i \mid \varphi_i$ is abstractable as $v'_{i,1} \mid \varphi'_{i,1} \vee \ldots \vee v'_{i,k_i} \mid \varphi'_{i,k_i}$. The following holds for any initial states $[u] \in \mathbb{C}_{\mathcal{R}}$, $[u!] = [u!_{\vec{E} \cup \vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}] \in \mathbb{C}_{\mathcal{R}/G}$:

$$\mathbb{C}_{\mathcal{R}}, [u] \models_{S4} \Diamond(v_1 \mid \varphi_1 \vee \ldots \vee v_m \mid \varphi_m) \;\Rightarrow\; \mathbb{C}_{\widehat{\mathcal{R}/G}}, [u!] \models_{S4} \Diamond \bigvee_{1 \leqslant i \leqslant m} (v'_{i,1} \mid \varphi'_{i,1} \vee \ldots \vee v'_{i,k_i} \mid \varphi'_{i,k_i})$$

Proof: The proof follows as an immediate corollary of **Theorem 2** as follows. $\mathbb{C}_{\mathcal{R}}$ is a Kripke structure on state predicates $\Pi = \{u, v_1 \mid \varphi_1, \ldots, v_m \mid \varphi_m\}$. $\mathbb{C}_{\widehat{\mathcal{R}/G}}$ is a Kripke structure on state predicates $\Pi' = \{u!\} \cup \bigcup_{1 \leqslant i \leqslant m} \{v'_{i,1} \mid \varphi'_{i,1}, \ldots, v'_{i,k_i} \mid \varphi'_{i,k_i}\}$. The function $H : \Pi \to \mathcal{P}_{fin}(\Pi')$ maps u to $u!$ and each $v_i \mid \varphi_i$ to $\{v'_{i,1} \mid \varphi'_{i,1}, \ldots, v'_{i,k_i} \mid \varphi'_{i,k_i}\}$, $1 \leqslant i \leqslant m$. The unique surjective Σ-homomorphism

$$[\_!_{\vec{E} \cup \vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}] : \mathbb{C}_{\Sigma/\vec{E},B} \to \mathbb{C}_{\Sigma/\vec{E},\vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}$$

and H define an H-homomorphism of Kripke structures from $\mathbb{C}_{\mathcal{R}}$ to $\mathbb{C}_{\widehat{\mathcal{R}/G}}$ because condition (i) is guaranteed by **Corollary 1**, and condition (ii) is guaranteed by **Proposition 2**. □

3 LTL Properties and Strong Simulation Maps

Given a Kripke structure $\mathcal{K} = (K, \to_{\mathcal{K}}, \_{\mathcal{K}})$ any subset $A \subseteq K$ defined a Kripke structure $\mathit{Reach}_{\mathcal{K}}(A) = (\mathit{Reach}_{\mathcal{K}}(A), \to_{\mathit{Reach}_{\mathcal{K}}(\mathcal{A})}, \_{\mathit{Reach}_{\mathcal{K}}(A)})$, where, by definition, (i) $\mathit{Reach}_{\mathcal{K}}(A) = \{k' \in K \mid \exists k \in K \;\; s.t. \;\; k \to^{*}_{\mathcal{K}} k'\}$, (ii) $\to_{\mathit{Reach}_{\mathcal{K}}(\mathcal{A})} = \to_{\mathcal{K}} \cap \mathit{Reach}_{\mathcal{K}}(A)^2$, and (iii) $\forall p \in \Pi$, $p_{\mathit{Reach}_{\mathcal{K}}(A)} = p_{\mathcal{K}} \cap \mathit{Reach}_{\mathcal{K}}(A)$. That is, $\mathit{Reach}_{\mathcal{K}}(A)$ is just the *restiction* of $\mathcal{K}$ to the states *reachable* from the set of initial states A. The main theorem about LTL properties of strong H-simulation maps is the following:

Theorem 3. For any H-simulation map of Kripke structures $h : \mathcal{K} \to \mathcal{K}'$ on Π and Π', such that $h : \mathcal{K} \to \mathcal{K}'|_H$ is a strong simulation map, $\Pi = \{p_1, \ldots, p_n\}$, $H(p_i) = \{q_{i,j_1}, \ldots, q_{i,j_{r(i)}}\} \subseteq \Pi'$, $1 \leqslant i \leqslant n$, $h : \mathcal{K} \to \mathcal{K}'|_H$ a strong simulation map, and sets of initial states $A \subseteq K$ and $A' \subseteq K'$ such that $h[A] \subseteq A'$ and the Kripke structure $\mathit{Reach}_{\mathcal{K}}(A)$ is deadlock-free, then the following implication holds for any LTL formula $\varphi \in LTL(\Pi)$:

$$\mathcal{K}', A' \models_{LTL} H(\varphi) \;\;\Rightarrow\;\; \mathcal{K}, A \models_{LTL} \varphi.$$

where $H(\varphi)$ is inductively defined as follows: (i) $H(p_i) = (q_{i,j_1} \vee \ldots \vee q_{i,j_{r(i)}})$, (ii) $H(\neg\psi) = \neg H(\psi)$, (iii) $H(\psi_1 \vee \psi_2) = H(\psi_1) \vee H(\psi_2)$, (iv) $H(\bigcirc\psi) = \bigcirc H(\psi)$, and (iv) $H(\psi_1 \mathcal{U} \psi_2) = H(\psi_1) \mathcal{U} H(\psi_2)$.

Proof. First of all, an easy structural induction on $\varphi \in LTL(\Pi)$ proves that $\mathcal{K}', A' \models_{LTL} H(\varphi)$ iff $\mathcal{K}'|_H, A' \models_{LTL} \varphi$. The second observation is that $\mathcal{K}, A \models_{LTL} \varphi$ iff $\mathit{Reach}_{\mathcal{K}}(A), A \models_{LTL} \varphi$. So, we just need to prove that

$$\mathcal{K}'_H, A' \models_{LTL} \varphi \;\;\Rightarrow\;\; \mathit{Reach}_{\mathcal{K}}(A), A \models_{LTL} \varphi.$$

The proof is by contradiction. Suppose $\mathit{Reach}_{\mathcal{K}}(A), A \not\models_{LTL} \varphi$. This exactly means that there is a state $a \in A$ and an infinite path $\pi \in \mathit{Paths}(\mathit{Reach}_{\mathcal{K}}(A)^{\bullet})_a$ such that $\pi; \mathit{preds} \not\models_{LTL} \varphi$. But since $Reach_{\mathcal{K}}(A)$ is deadlock-free, $\pi \in Paths(Reach_{\mathcal{K}}(A))_a$, and therefore $\pi; h \in Paths(\mathcal{K}'_H)_{h(a)}$, and, a fortiori, $\pi; h \in Paths(\mathcal{K}'^{\bullet}_H)_{h(a)}$. But since $h : \mathcal{K} \to \mathcal{K}'|_H$ is a strong simulation map, for each $a' \in A$ we must have $preds(a') = preds(h(a'))$, which forces the trace equality $\pi; h; preds = \pi; preds$ and therefore that $\pi; h; preds \not\models_{LTL} \varphi$ with $h(a) \in A'$, contradicting the hypothesis $\mathcal{K}'_H, A' \models_{LTL} \varphi$. $\square$

Remark. Note that in general the above theorem will not hold if $Reach_{\mathcal{K}}(A)$ isn't deadlock-free. For example, we may have $\mathcal{K}$ with states a, b, c, d and transitions $a \to b$, $a \to c$, $c \to d$ and $d \to c$, $A = \{a, b, c, d\}$, $\mathcal{K}'$ with states $a, \{b, c\}, d$ and transitions $a \to \{b, c\}$, $\{b, c\} \to d$ and $d \to \{b, c\}$ and $A' = \{a, \{b, c\}, d\}$. Let h be the identity on a and d and map b and c to $\{c, d\}$. Then, the infinite path $\pi = a \to b \to b \to b \ldots$ in $\mathcal{K}^{\bullet} = Reach_{\mathcal{K}}(A)^{\bullet}$ has no corresponding infinite path of the form $\pi; h$ in $\mathcal{K}'^{\bullet} = \mathcal{K}'$, so the above proof's argument falls apart.

4 Using Equational Abstractions in LTL Model Checking

The above requirements and results in §3 on the use of Kripke H-simulation maps to prove LTL properties have a direct bearing on how to do so using equational abstractions, both for symbolic and for explicit-state model checking. Since symbolic LTL model checking will be discussed in Lecture 27, I will focus in what follows on the explicit-state case supported by Maude's LTL model checker.

First of all, the assumptions and results about model checking of modal logic properties that culminated in **Proposition 4** above remain a basic requirement: in $\widehat{\mathcal{R}/G}$ both state predicates and rules in the topmost and admissible $\mathcal{R}$ should be *G-abstractable.* But there are three additional issues to be discussed:

1. In hindsight, the abstraction of a state predicate $u \mid \varphi$ in $\mathcal{R}$ by is G-abstraction $u'_1 \mid \varphi'_1 \vee \ldots \vee u'_n \mid \varphi'_n$ defines what in §3 has been called an H-simulation map between the Kripke structures $\mathbb{C}_{\mathcal{R}}$ and $\mathbb{C}_{\widehat{\mathcal{R}/G}}$. However, in LTL we must explictly *choose* state predicate *names* Π. The easiest and most natural choice it to use the *same* Π for both $\mathbb{C}_{\mathcal{R}}$ and $\mathbb{C}_{\widehat{\mathcal{R}/G}}$ in such a way that if $p \in \Pi$ is interpreted as $u \mid \varphi$ in $\mathcal{R}$, it is instead intepreted as $u'_1 \mid \varphi'_1 \vee \ldots \vee u'_n \mid \varphi'_n$ in $\mathbb{C}_{\widehat{\mathcal{R}/G}}$. In practical terms what this means is that the definion of p in $\mathbb{C}_{\mathcal{R}}$ by the conditional equation $u \models p = true \;\; if \;\; \varphi$ is instead done in $\mathbb{C}_{\widehat{\mathcal{R}/G}}$ by the equations $\{u'_i \models p = true \;\; if \;\; \varphi'_i\}_{1 \leqslant i \leqslant n}$. In the notation of §3 sharing the same Π just means that $\mathbb{C}_{\widehat{\mathcal{R}/G}}$ is implicitly of the form $\mathbb{C}_{\widehat{\mathcal{R}/G}}|_H$, since we could have defined each $u'_i \mid \varphi'_i$ as a separate predicate $p'_i \in \Pi'$ and could have then related Π and Π' by an explicit H mapping each p to its G-abstraction $\{p'_1, \ldots, p'_n\}$ to get $\mathbb{C}_{\widehat{\mathcal{R}/G}}|_H$.

2. A second issue is that we want the surjective simulation map of Kripke structures
$$[\_!_{\vec{E} \cup \vec{E}'_{\Omega+}/B \cup B'_{\Omega+}}] : \mathbb{C}^{\Pi}_{\mathcal{R}} \to \mathbb{C}^{\Pi}_{\widehat{\mathcal{R}/G}}$$
to be *strong*, which is a non-trivial matter. A practical method to achieve this property is explained in detail below and is illustrated by an example in Lecture 26.

3. A third important issue, clearly highlighted in §3, is that if we want to use $\mathbb{C}_{\widehat{\mathcal{R}/G}}$ to prove LTL properties about $\mathbb{C}_{\mathcal{R}}$ from an initial state $[u] \in \mathbb{C}_{\mathcal{R}}$ and $\mathbb{C}_{\mathcal{R}}$ itself is not deadlock-free, we need to either: (i) prove that the set of states reachable from $[u]$ is deadlock

free, or (ii) make $\mathbb{C}_{\mathcal{R}}$ itself deadlock free, which is quite easy to do. Suppose that f is the only constructor of the topmost sort *State*. We just add to $\mathcal{R}$ the rule:

$$f(x_1, \ldots, x_n) \to f(x_1, \ldots, x_n) \;\; \mathit{if} \;\; \mathit{enabled}(f(x_1, \ldots, x_n)) \neq \mathit{true}$$

where *enabled* is defined in the usual way using the lefthand sides of the rules in $\mathcal{R}$.

The only pending issue is how to ensure that the map of Kripke structures $[\_!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}] : \mathbb{C}^{\Pi}_{\mathcal{R}} \to \mathbb{C}^{\Pi}_{\widehat{\mathcal{R}/G}}$ is *strong*. The method embodied in the following proposition gives us a way to do that.

Proposition 5. Assume that all rules in the admissible topmost theory $\mathcal{R} = (\Sigma, E \cup B, R)$ are G-abstractable, $\widehat{\mathcal{R}/G} = (\Sigma, E \cup E'_{\Omega+} \cup B \cup B'_{\Omega+}, \widehat{R})$ is admissible, $\mathcal{R}$ has an FVP constructor subtheory $E_{\Omega+} \cup B_{\Omega+}$, $G = E'_{\Omega+} \cup B'_{\Omega+}$, and $E'_{\Omega+} \cup E'_{\Omega+} \cup B_{\Omega+} \cup B'_{\Omega+}$ is also FVP. Let $\Pi = \{p_1, \ldots, p_n\}$ be state predicate symbols and let $\mathcal{R}^{\Pi}$ extend $\mathcal{R}$ and `BOOL` by adding: (1) a new sort *Prop* with constants $p_1, \ldots, p_n$, (2) an operator $\_ \models \_ : \mathit{State}\,\mathit{Prop} \to \mathit{Bool}$, and (3) equations E_{Π} of either the form $u \models p_i = \mathit{true} \; \mathit{if} \; \varphi$, or $v \models p_i = \mathit{false} \; \mathit{if} \; \psi$ for $1 \leqslant i \leqslant n$ (there can be *more than one equation* defining p_i in this way for the positive and/or the the negative cases). Furthermore, for all equations in E_{Π} their associated $u \mid \varphi$ (resp. $v \mid \psi$) are constrained constructor terms, and: (i) the equations $E \cup E_{\Pi} \cup B$ are ground convergent and protect `BOOL`, and (ii) all $u \mid \varphi$ (resp. $v \mid \psi$) associated to positive (resp. negative) equations in E_{Π} are G-abstractable by $u'_1 \mid \varphi'_1 \vee \ldots \vee u'_k \mid \varphi'_k$ (resp. by $v'_1 \mid \psi'_1 \vee \ldots \vee v'_r \mid \psi'_r$).

Let $\widehat{\mathcal{R}/G}^{\Pi}$ extend $\widehat{\mathcal{R}/G}$ and `BOOL` by adding (1) and (2) as above, and (3) add to the equations $\mathit{abs}(E_{\Pi})$ obtained by adding to E_{Π}: for each equation $u \models p_i = \mathit{true} \; \mathit{if} \; \varphi$ in E_{Π}, the equations $\{u'_j \models p_i = \mathit{true} \; \mathit{if} \; \varphi'_j\}_{1 \leqslant j \leqslant k}$ (resp. for each equation $v \models p_i = \mathit{false} \; \mathit{if} \; \psi$ in E_{Π}, the equations $\{v'_l \models p_i = \mathit{false} \; \mathit{if} \; \psi'_l\}_{1 \leqslant l \leqslant r}$). Then, if the equations $E \cup G \cup \mathit{abs}(E_{\Pi}) \cup B$ are ground convergent and protect `BOOL`, then the map of Kripke structures $[\_!_{\vec{E} \cup \vec{E'}_{\Omega+}/B \cup B'_{\Omega+}}] : \mathbb{C}^{\Pi}_{\mathcal{R}} \to \mathbb{C}^{\Pi}_{\widehat{\mathcal{R}/G}}$ is strong.

Proof: By **Corollary 1**, condition (i) in the definition of simulation map of Kripke structures holds. We just need to prove that for each state $[u] \in \mathbb{C}^{\Pi}_{\mathcal{R}}$ and $p \in \Pi$, $(u \models p)!_{\vec{E} \cup \vec{E}_{\Pi}/B} = (u \models p)!_{\vec{E} \cup \vec{E'}_{\Omega+} \cup \vec{abs(E)}_{\Pi}/B \cup B'_{\Omega+}}$. But since the equations $E \cup E_{\Pi} \cup B$ are ground convergent and protect `BOOL`, either: (i) $(u \models p)!_{\vec{E} \cup \vec{E}_{\Pi}/B} = \mathit{true}$, or (ii) $(u \models p)!_{\vec{E} \cup \vec{E}_{\Pi}/B} = \mathit{false}$. And since the equations $E \cup G \cup \mathit{abs}(E_{\Pi}) \cup B$ are ground convergent and protect `BOOL`, by the ground Church-Rosser property in case (i) we must have $(u \models p)!_{\vec{E} \cup \vec{E'}_{\Omega+} \cup \vec{abs(E)}_{\Pi}/B \cup B'_{\Omega+}} = \mathit{true}!_{\vec{E} \cup \vec{E'}_{\Omega+} \cup \vec{abs(E)}_{\Pi}/B \cup B'_{\Omega+}} = \mathit{true}$, and likewise for case (ii), proving strongness, as desired. □

For ease of reference, the Main Theorem on LTL model checking using equational abstractions in pg. 18 of Lecture 26 is here relabeled as **Proposition 6**.

Proposition 6. Let $\mathcal{R}$ be topmost admissible, and $\mathcal{R}$ is deadlock-free (or at least the states reachable from $[u] \in \mathbb{C}^{\Pi}_{\Sigma/\vec{E},B}$ are so), have an admissible equational abstraction $\widehat{\mathcal{R}/G}$, and satisfy all the assumptions in **Proposition 5**. Then, for each state $[u] \in \mathbb{C}^{\Pi}_{\mathcal{R}}$ and $\varphi \in LTL(\Pi)$ the following implication holds:

$$\mathbb{C}_{\widehat{\mathcal{R}/G}}, [u!] \models_{LTL} \varphi \;\Rightarrow\; \mathbb{C}_{\mathcal{R}}, [u] \models_{LTL} \varphi.$$

where $[u!]$ abbreviates $[u!_{\vec{E}\cup\vec{E'}_{\Omega+}/B\cup B'_{\Omega+}}]$.

Proof: By **Proposition 5**, the map of Kripke structures $[\_!_{\vec{E}\cup\vec{E'}_{\Omega+}/B\cup B'_{\Omega+}}] : \mathbb{C}^{\Pi}_{\mathcal{R}} \to \mathbb{C}^{\Pi}_{\widehat{\mathcal{R}/G}}$ is strong. The theorem now follows as a corollary of **Theorem 3** by choosing $A = \{[u]\}$, $A' = \{[u!]\}$, and $H : \Pi \ni p \mapsto \{p\} \in \mathcal{P}_{fin}(\Pi)$. $\square$